

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-115838

(43)Date of publication of application : 18.04.2003

(51)Int.Cl.

H04L 9/32

(21)Application number : 2002-186588

(71)Applicant : MATSUSHITA ELECTRIC IND CO  
LTD

(22)Date of filing : 26.06.2002

(72)Inventor : NAKANO TOSHIHISA  
OMORI MOTOJI  
TATEBAYASHI MAKOTO

(30)Priority

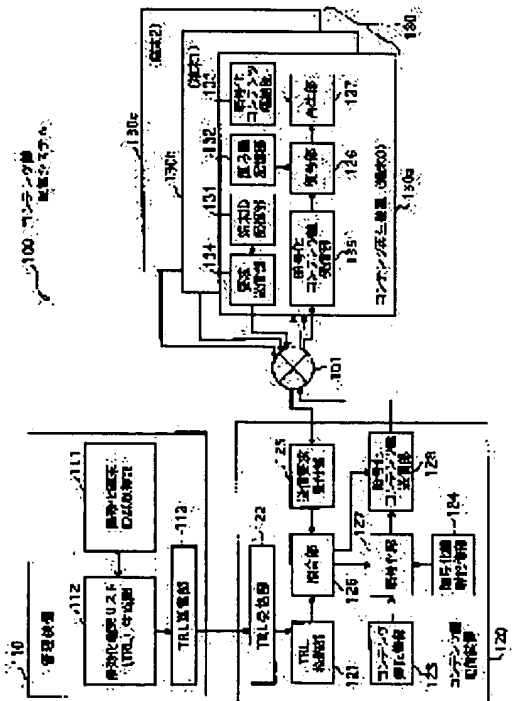
Priority number : 2001233223 Priority date : 01.08.2001 Priority country : JP

## (54) ENCRYPTED DATA DELIVERY SYSTEM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide technology for suppressing the data amount of information (TRL) for specifying a plurality of terminals and a terminal to be invalidated in a system composed of a plurality of terminals, a distributor for delivering data only to terminals except for the terminal to be invalidated and a management device for generating the TRL.

**SOLUTION:** A management device 110 generates the TRL composed of data expressing the terminal ID of all invalidated terminals having a common bit stream in one part of the terminal ID only with the position and value of the bit stream in one part and transmits the TRL to a contents key distributor 120. Each of terminals 130 holds the terminal ID containing a maker class and a serial number or the like and the distribution of the contents key is requested by sending the terminal ID to the contents key distributor 120. While referring to the TRL, the contents key distributor 120 decides whether the terminal ID sent from the terminal is the terminal ID of the invalidated terminal or not and when the sent terminal ID is not the terminal ID of the invalidated terminal, the contents key is enciphered and transmitted to that terminal.



THIS PAGE BLANK (USPC)

16 17 18

19 20 21 22 23 24

---

**LEGAL STATUS**

[Date of request for examination] 07.02.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-115838

(P2003-115838A)

(43) 公開日 平成15年4月18日 (2003.4.18)

(51) Int.Cl.<sup>7</sup>

H 0 4 L 9/32

識別記号

F I

H 0 4 L 9/00

テーマコード(参考)

6 7 3 B 5 J 1 0 4

審査請求 未請求 請求項の数36 O L (全 30 頁)

(21) 出願番号 特願2002-186588(P2002-186588)

(22) 出願日 平成14年6月26日 (2002.6.26)

(31) 優先権主張番号 特願2001-233223(P2001-233223)

(32) 優先日 平成13年8月1日 (2001.8.1)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 中野 稔久

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 大森 基司

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗

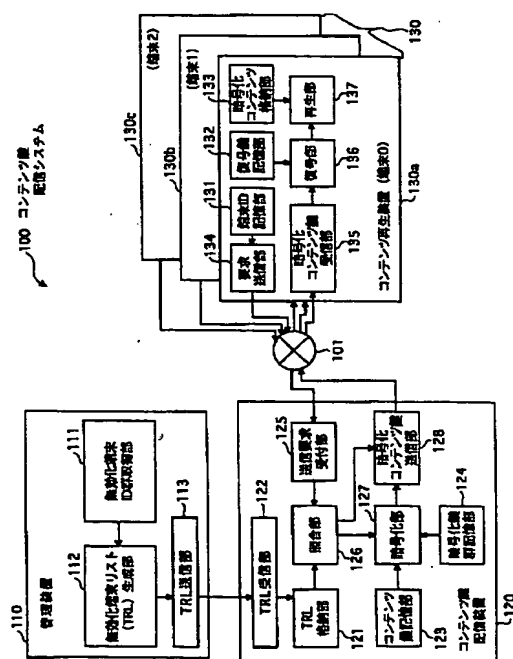
最終頁に続く

(54) 【発明の名称】 暗号化データ配信システム

(57) 【要約】

【課題】 複数の端末と、無効化すべき端末を特定する情報 (TRL) を取得して無効化すべき端末以外の端末に対してのみデータを配信する配信装置と、TRLを生成する管理装置から構成されるシステムにおけるTRLのデータ量を抑える技術を提供する。

【解決手段】 管理装置110は、端末ID中の一部のビット列が共通な全ての無効化端末の端末IDを、その一部のビット列の位置及び値のみで表現したデータからなるTRLを生成してコンテンツ鍵配信装置120に送信する。各端末130はメーカー種別やシリアル番号等を含む端末IDを保持しており、コンテンツ鍵配信装置120に対し端末IDを送ってコンテンツ鍵の配信要求を行う。コンテンツ鍵配信装置120は、TRLを参照し、端末から送られた端末IDが無効化端末の端末IDか否かを判定し、送られた端末IDが無効化端末の端末IDでなければその端末にコンテンツ鍵を暗号化して送信する。



## 【特許請求の範囲】

【請求項1】 暗号通信装置と、自端末装置を識別可能な所定ビット数のビット列なる端末識別子を、当該暗号通信装置に送信する機能を有する複数の端末装置と、無効化すべき端末装置を特定するものとして1以上の端末識別子を示す無効化端末特定情報を生成する管理装置とを備える暗号通信システムであって、前記管理装置は、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを有し、前記暗号通信装置は、前記管理装置により出力された前記無効化端末特定情報を取得する無効化端末特定情報取得手段と、端末装置から端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、一方、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを有することを特徴とする暗号通信システム。

【請求項2】 前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて1組以上含んでおり、端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各位置情報について、前記端末識別子受信手段により受信された端末識別子中の当該位置情報により特定されるビット位置に所在

する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項1記載の暗号通信システム。

【請求項3】 前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列である代表値情報と、所定ビット数のマスクフラグとを対応付けて1組以上含んでおり、端末識別子中の部分のうち各マスクフラグにおけるビット値が1である部分の値が、当該マスクフラグに対応する代表値情報における当該部分の値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各マスクフラグについて、前記端末識別子受信手段により受信された端末識別子と当該マスクフラグとの論理積と、当該マスクフラグに対応する代表値情報と当該マスクフラグとの論理積とが一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項1記載の暗号通信システム。

【請求項4】 前記無効化端末特定情報生成手段は、前記無効化端末特定情報に所定ビット数の孤立値情報を含めて生成し、前記無効化端末特定情報は、更に前記孤立値情報と同一の値を有する端末識別子をも、無効化すべき端末装置として特定する情報であり、前記判定手段は更に、前記端末識別子受信手段により受信された端末識別子と、前記無効化端末特定情報に含まれる孤立値情報とが一致する場合にも、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項3記載の暗号通信システム。

【請求項5】 前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、ビット桁数を示す有効上位桁情報と、当該ビット桁数分のビット列の値を示す値情報とを対応付けて1組以上含んでおり、端末識別子中の最上位ビットから各有効上位桁情報により示されるビット桁数分のビット列の値が、当該有効上位桁情報に対応する値情報で示される値と同一である全

ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、

前記判定手段は、

前記無効化端末特定情報に含まれる各有効上位桁情報について、前記端末識別子受信手段により受信された端末識別子中の最上位ビットから当該有効上位桁情報により示されるビット桁数分のビット列の値が、当該有効上位桁情報に対応する値情報で示される値と一致するか否かを検査し、

当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項1記載の暗号通信システム。

【請求項6】 前記管理装置は、無効化すべき全ての端末装置の端末識別子を取得する端末識別子取得手段を有し、

前記無効化端末特定情報生成手段は、前記所定ビット数をNとすると、前記端末識別子取得手段により取得された端末識別子のうち最上位ビットからXビットの値が同一である端末識別子の個数が2の(N-X)乗であるという条件を満たすXの値を1以上特定し、各Xの値について、当該条件に係る2の(N-X)乗個の端末識別子を、Xなるビット桁数を示す有効上位桁情報と、当該端末識別子の最上位ビットからXビットの部分のビット列の値を示す値情報とをもって包括的に表現したデータ形式を用いて前記無効化端末特定情報を生成することを特徴とする請求項5記載の暗号通信システム。

【請求項7】 前記各端末装置は、複数の製造者のうちのいずれかにより製造されたものであり、

前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すことを特徴とする請求項6記載の暗号通信システム。

【請求項8】 前記各端末装置を識別する各端末識別子は、当該端末識別子中の前記製造者を示すビット列に続く上位の所定数のビット列で、当該端末装置が如何なる種類の製品に属するかを示すことを特徴とする請求項7記載の暗号通信システム。

【請求項9】 前記複数の端末装置は各々固有の復号鍵を保持しており、更にコンテンツ鍵で暗号化されたコンテンツである暗号化コンテンツを自端末装置内部に格納可能であり、

前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、

前記暗号通信装置は、

全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段と、

前記コンテンツ鍵を記憶するコンテンツ鍵記憶手段とを

有し、

前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行い、

前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて前記コンテンツ鍵を暗号化して送信し、

前記端末装置は、

暗号通信装置から送信された暗号化済みのコンテンツ鍵を自端末装置固有の前記復号鍵を用いて復号する復号手段と、

前記暗号化コンテンツが自端末装置内部に格納されている場合において前記復号手段により復号されたコンテンツ鍵を用いて当該暗号化コンテンツを復号して再生する再生手段とを有することを特徴とする請求項7記載の暗号通信システム。

20 【請求項10】 前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、

所定ビット数のビット列中の一部分の値及び当該部分を特定する包括情報を1以上含み、かつ、所定ビット数の例外情報を1以上含んでおり、

端末識別子中の部分のうち各包括情報により特定される部分が当該包括情報により特定される値と同一である全ての端末識別子のうちから、前記各例外情報と同値である端末識別子を除いたものの全てを、無効化すべき端末装置として特定する情報であり、

30 前記判定手段は、

前記端末識別子受信手段により受信された端末識別子が、前記無効化端末特定情報に含まれるいずれかの包括情報により特定される部分において当該包括情報により特定される値と一致するか否かを検査し、

当該検査において一致した場合には、当該受信された端末識別子が前記無効化端末特定情報に含まれるいずれかの例外情報と同値である場合を除いて、当該端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項1記載の暗号通信システム。

40 【請求項11】 前記管理装置は、無効化すべき全ての端末装置の端末識別子を取得する端末識別子取得手段を有し、

前記無効化端末特定情報生成手段は、前記所定ビット数をNとすると、

前記端末識別子取得手段により取得されたいずれかの端末識別子の最下位ビットのみ反転したNビットのビット列であって、当該端末識別子取得手段により取得された他のいずれかの端末識別子とも値が同一でないという条

50

件を満たすビット列を、前記例外情報と定めるとともに、当該ビット列を端末識別子とみなし、前記端末識別子取得手段により取得された端末識別子及び前記みなした端末識別子のうち、最上位ビットからXビットの値が同一である端末識別子の個数が2の(N-X)乗であるという条件を満たすXの値で、かつ、N未満であるXの値を、1以上特定し、特定した各Xの値について、当該Xの値と、当該条件に係る2の(N-X)乗個の端末識別子の最上位ビットからXビットの部分のビット列の値とを特定する情報を前記包括情報と定めることにより前記無効化端末特定情報を生成することを特徴とする請求項10記載の暗号通信システム。

【請求項12】 前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すことを特徴とする請求項11記載の暗号通信システム。

【請求項13】 前記複数の端末装置は各々固有の復号鍵を保持しており、更にコンテンツ鍵で暗号化されたコンテンツである暗号化コンテンツを自端末装置内部に格納可能であり、前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、前記暗号通信装置は、全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段と、前記コンテンツ鍵を記憶するコンテンツ鍵記憶手段とを有し、前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行い、前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて前記コンテンツ鍵を暗号化して送信し、前記端末装置は、暗号通信装置から送信された暗号化済みのコンテンツ鍵を自端末装置固有の前記復号鍵を用いて復号する復号手段と、前記暗号化コンテンツが自端末装置内部に格納されている場合において前記復号手段により復号されたコンテンツ鍵を用いて当該暗号化コンテンツを復号して再生する再生手段とを有することを特徴とする請求項12記載の暗号通信システム。

【請求項14】 前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、前記各端末装置を識別する各端末識別子は、当該端末識

別子中の所定範囲のビット列で当該端末装置の製造者を示すことを特徴とする請求項1記載の暗号通信システム。

【請求項15】 前記複数の端末装置は各々固有の復号鍵を保持しており、

前記暗号通信装置は、全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段を有し、

前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて通信データを暗号化して送信し、

前記端末装置は、暗号通信装置から送信された通信データを自端末装置固有の前記復号鍵を用いて復号することを特徴とする請求項1記載の暗号通信システム。

【請求項16】 前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、

前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行うことを特徴とする請求項1記載の暗号通信システム。

【請求項17】 前記出力手段は、記録媒体を装着可能な装着部を有し、装着された記録媒体に前記無効化端末特定情報を記録することにより前記出力を行い、

前記無効化端末特定情報取得手段は、前記記録媒体を装着可能であり、装着された記録媒体から前記無効化端末特定情報を読み出すことにより前記取得を行うことを特徴とする請求項1記載の暗号通信システム。

【請求項18】 複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき1以上の各端末装置の各端末識別子を示す無効化端末特定情報を生成する管理装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、

生成された前記無効化端末特定情報を出力する出力手段とを備えることを特徴とする管理装置。

【請求項19】 前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて1組以上含んでおり、

端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と



同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であることを特徴とする請求項18記載の管理装置。

【請求項20】 前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、前記各端末装置を識別する各端末識別子は、当該端末識別子中の所定範囲のビット列で当該端末装置の製造者を示すことを特徴とする請求項19記載の管理装置。

【請求項21】 複数の端末装置のうち自端末装置を識別可能な所定ビット数のビット列なる端末識別子を保持する各端末装置との間で通信を行う暗号通信装置であって、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて構成され、無効化すべき端末装置を特定するためのものとして1以上の各端末装置の各端末識別子を示した無効化端末特定情報を外部から取得する無効化端末特定情報取得手段と、

端末装置から、当該端末装置が保持する端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、

前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、

前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを備えることを特徴とする暗号通信装置。

【請求項22】 前記無効化端末特定情報取得手段により取得される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて1組以上含んでおり、

端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、

前記無効化端末特定情報に含まれる各位置情報について、前記端末識別子受信手段により受信された端末識別子中の当該位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項21記載の暗号通信装置。

【請求項23】 複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成方法であって、

前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップとを含むことを特徴とする情報生成方法。

【請求項24】 前記生成ステップは、前記所定ビット数をNとすると、前記端末識別子取得ステップにより取得された端末識別子のうち最上位ビットからXビットの値が同一である端末識別子の個数が2の(N-X)乗であるという条件を満たすXの値を1以上特定し、各Xの値について、Xなるビット桁数を示す有効上位桁情報と、当該端末識別子の最上位ビットからXビットの部分のビット列の値を示す値情報とを対応付けて、対応付けた有効上位桁情報と値情報との全ての組を構成要素とする前記無効化端末特定情報を生成することを特徴とする請求項23記載の情報生成方法。

【請求項25】 前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すことを特徴とする請求項24記載の情報生成方法。

【請求項26】 前記生成ステップは、前記所定ビット数をNとすると、前記端末識別子取得ステップにより取得されたいずれかの端末識別子の最下位ビットのみ反転したNビットのビット列であって、当該端末識別子取得ステップにより取得された他のいずれかの端末識別子とも値が同一でないという条件を満たすビット列を、例外情報として定めるとともに、当該ビット列を端末識別子とみなし、前記端末識別子取得ステップにより取得された端末識別子及び前記みなした端末識別子のうち、最上位ビットか

らXビットの値が同一である端末識別子の個数が2の(N-X)乗であるという条件を満たすXの値で、かつ、N未満であるXの値を、1以上特定し、特定した各Xの値について、当該Xの値と、当該条件に係る2の(N-X)乗個の端末識別子の最上位ビットからXビットの部分のビット列の値と対応付けて、対応付けた値の全ての組と前記例外情報とを構成要素とする前記無効化端末特定情報を生成することを特徴とする請求項2記載の情報生成方法。

【請求項27】 前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、

前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すことを特徴とする請求項26記載の情報生成方法。

【請求項28】 複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成処理をコンピュータに実行させるためのプログラムであって、

前記情報生成処理は、

前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップを含むことを特徴とするプログラム。

【請求項29】 複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成処理をコンピュータに実行させるためのプログラムを記録した記録媒体であって、

前記情報生成処理は、

前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップを含むことを特徴とする記録媒体。

【請求項30】 端末装置から送信される端末識別子に基づいて当該端末装置が無効化すべき端末装置であるかを判定する判定処理をコンピュータに実行させるためのプログラムであって、

前記判定処理は、

端末装置から送信される所定ビット数の端末識別子を受信する端末識別子受信ステップと、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、無効化すべき1以上の端末装置の各端末識別子を特定する無効化端末特定情報を取得する無効化端末特定情報取得ステップと、

10 前記端末識別子受信ステップにより受信された端末識別子が、前記無効化端末特定情報により特定される何れかの端末識別子と一致するか否かを判定する判定ステップを含むことを特徴とするプログラム。

【請求項31】 端末装置から送信される端末識別子に基づいて当該端末装置が無効化すべき端末装置であるかを判定する判定処理をコンピュータに実行させるためのプログラムを記録した記録媒体であって、

前記判定処理は、

端末装置から送信される所定ビット数の端末識別子を受信する端末識別子受信ステップと、

20 前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、無効化すべき1以上の端末装置の各端末識別子を特定する無効化端末特定情報を取得する無効化端末特定情報取得ステップと、

前記端末識別子受信ステップにより受信された端末識別子が、前記無効化端末特定情報により特定される何れかの端末識別子と一致するか否かを判定する判定ステップを含むことを特徴とする記録媒体。

30 【請求項32】 無効化端末特定データを記録したコンピュータ読み取り可能な記録媒体であって、

前記無効化端末特定データは、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を特定するために、

前記所定ビット数のビット列中の一部分の値を特定するための部分特定情報を記録した端末識別子特定フィールドを有し、

40 当該部分特定情報により、当該部分が当該値と同一である全ての端末識別子を包括的に表現していることを特徴とする記録媒体。

【請求項33】 前記端末識別子特定フィールドは、所定ビット数のビット列中の一部分の値を示す値情報を記録した値情報フィールドと、

前記ビット列中における前記部分のビット位置を特定するための位置情報を記録した位置情報フィールドとを対応付けてなる組を1組以上含んで構成され、

50 前記無効化端末特定データは、端末識別子中の部分的なビット列であって前記各位置情報フィールド内の各位置情報により特定されるビット位

置に所在する部分的なビット列の値が、当該位置情報が記録された位置情報フィールドに対応する値情報フィールドに記録された値情報で示される値と、同一である全ての端末識別子それぞれを、無効化すべき各端末装置の端末識別子として特定するデータであることを特徴とする請求項32記載の記録媒体。

【請求項34】 前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、

前記各端末装置を識別する各端末識別子は、当該端末識別子中の所定範囲のビット列で当該端末装置の製造者を示すことを特徴とする請求項33記載の記録媒体。

【請求項35】 複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を特定するために、前記所定ビット数のビット列中の一部分の値を特定するための部分特定情報を記録した端末識別子特定フィールドを有し、

当該部分特定情報により、当該部分が当該値と同一である全ての端末識別子を包括的に表現していることを特徴とする無効化端末特定データ。

【請求項36】 暗号通信装置と、当該暗号通信装置に所定ビット数の鍵識別子を送信する端末装置と、無効化すべき1以上の各鍵識別子を特定する無効化鍵識別子特定情報を生成する管理装置とを備える暗号通信システムであって、

前記管理装置は、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての鍵識別子を包括的に表現するデータ形式を用いて、前記無効化鍵識別子特定情報を生成する無効化鍵識別子特定情報生成手段と、

生成された前記無効化鍵識別子特定情報を出力する出力手段とを有し、

前記暗号通信装置は、

前記管理装置により出力された前記無効化鍵識別子特定情報を取得する無効化鍵識別子特定情報取得手段と、

端末装置から鍵識別子を受信する鍵識別子受信手段と、

前記鍵識別子受信手段により受信された鍵識別子が、前記無効化鍵識別子特定情報により特定される何れかの鍵識別子と一致するか否かを判定する判定手段と、

前記受信された鍵識別子が前記無効化鍵識別子特定情報により特定される何れの鍵識別子とも一致しないと前記判定手段により判定された場合に限り、当該鍵識別子を送信した端末装置との間で、当該鍵識別子について固有な暗号化を施すことにより所定の通信を行う通信手段とを有することを特徴とする暗号通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、暗号通信システムに関し、特に、複数の端末装置のうち一部の端末装置が

らの要求には応えず、他の端末装置からの要求を受け付けてその端末装置に暗号化データを送信する暗号通信装置を含む暗号通信システムに関する。

【0002】

【従来の技術】 近年、インターネット関連技術の進展を背景として、インターネットを利用した電子商取引のシステム等が盛んに開発されている。電子商取引等におけるデータ通信では暗号技術が用いられる。例えば、通信相手の認証のためにしばしば公開鍵暗号系の暗号通信方式が用いられ、データを安全に配信するためにしばしば秘密鍵暗号系の暗号通信方式が用いられる。公開鍵暗号系及び秘密鍵暗号系の暗号技術については、文献「現代暗号理論」（池野信一、小山謙二、電子通信学会、1986年）に詳しく説明されている。

【0003】 公開鍵暗号系の暗号通信方式においては、一般に、公開鍵とそれを保有する人や物等の対応関係を証明すべく認証局と呼ばれる機関が発行した公開鍵証明書が、公開鍵に付加されて送信される。公開鍵証明書は基本的に秘密に扱われる必要のない公開情報である。なお、公開鍵と対になる秘密鍵は秘密に管理される必要がある。

【0004】 通常、公開鍵証明書は有効期間を持つが、公開鍵と対になる秘密鍵が事故や事件により暴露された場合又は暴露された疑いがある場合は、有効期間内であっても、その公開鍵証明書を無効化する必要がある。公開鍵証明書を無効化する方法として、文献「デジタル署名と暗号技術」（山田慎一郎訳、株式会社ピアソン・エデュケーション、189頁～196頁、1997年）には、証明書廃棄リスト（CRL: Certificate Revocation List）を公開する方法が示されている。このCRLには、無効化すべき全ての公開鍵証明書のシリアル番号が記載されており、CRLを利用して、CRLに記載されているシリアル番号の付いた公開鍵証明書を、無効とし使用できなくなるような機構が構築できる。

【0005】 ところで、著作権保護その他の目的から暗号化されている映画等のデジタルコンテンツを適切に利用すべきことが要求されるデジタルコンテンツ受信再生用の多数の端末装置に対し、その要求に応じて配信装置がデジタルコンテンツの復号用の鍵（以下、「コンテンツ鍵」という。）を配信するような配信サービスについて考えた場合、著作権保護等に鑑みれば、そのコンテンツ鍵の配信は、適切な端末装置に対してのみ行われるべきである。

【0006】 この配信サービスにおいて、端末装置は装置固有の秘密鍵を有し、鍵を配信する側の配信装置は、端末装置からコンテンツ鍵の配信要求とともに端末装置固有の端末識別子（端末ID）の通知を受けて、コンテンツ鍵に、その端末装置固有の秘密鍵でのみ復号可能な暗号化を施してその端末装置に送信するような配信方式等が用いられると考えられる。

【0007】この場合に、ある一部のメーカーが製造した端末装置における秘密鍵の実装方法に問題があることが判明した後は、そのメーカーの一群の端末装置に対してはコンテンツの鍵の配信を行わないようにする必要がある。また、端末装置におけるデジタルコンテンツのコピーを防止する等の機構について、ある一部のメーカーが製造した端末装置におけるその機構を無力化する方法が暴露された後は、そのメーカーの一群の端末装置に対してはコンテンツ鍵の配信を行わないようにする必要がある。

【0008】即ち、不正な状態となった端末装置に対してのコンテンツ鍵の配信を停止する必要がある。この必要性に応える方法として、配信サービスにおいて、配信装置は、端末装置からコンテンツ鍵の配信要求とともに端末IDを受け取ることとし、上述の公開鍵証明書のシリアル番号の代わりに無効化すべき全ての端末装置についての端末IDを記載しておくこととした変形版のCRL（以下、「TRL」（無効化端末リスト、Terminal Revocation List）という。）を用いることとし、受け取った端末IDがTRLに記載されていれば、その配信要求に応じず、記載されていない場合にのみ配信要求に応じて鍵を配信するというような方法が考えられる。

【0009】

【発明が解決しようとする課題】しかしながら、上述の方法では、無効化すべき端末装置が多数の場合に、その全ての端末装置の端末IDを記載するのでTRLのデータサイズが膨大になる。仮に、配信サービスの対象とする端末装置を、約40億台とし、端末IDを4バイト以上の固定長データとし、その端末装置のうちの1%を無効化すると想定した場合には、TRLは160メガバイト以上のデータサイズになる。

【0010】このため、配信サービスにおいて、多数の端末装置に対応するために、コンテンツ鍵を配信する側の配信装置を各地域等に分散して多数設けておき、1つの管理装置でTRLを生成してそのTRLにデジタル署名等を含め、公衆通信網等を通じて各配信装置に送信し、各配信装置ではそのTRLに基づいて端末装置への配信可否を判定するような運用形態を想定した場合、通信データ量が多く、また、各配信装置が保持すべきデータ量も多くなることから、この配信サービスは実用に耐えないものとなるおそれがある。

【0011】例えば、無効化すべき端末装置が増加する毎にTRLの送信を行うこととしたならば、通信データ量の多さにより、通信渋滞を招いてしまう。また、配信装置が端末装置から端末IDを伴い配信要求を受けた時点で管理装置に最新のTRLを要求して、TRLを受け取ってからTRLに基づき端末IDの照合を行うこととしたならば、配信装置がTRLの受信に多くの時間を要することにより、端末装置からの要求への応答が遅れてしまう。

【0012】そこで、本発明は、かかる問題に鑑みてなされたものであり、TRLを用いて一部の無効化すべき端末装置を除いた適切な端末装置に対してのみ、コンテンツ鍵を暗号化して配信する等の暗号通信に係るサービスを行う暗号通信システムであって、TRLのデータサイズを抑えて実用性を高めた暗号通信システムを、提供することを目的とする。

【0013】また、本発明は、上述の暗号通信システムの構築に資する各種技術を提供することを目的とする。

【0014】

【課題を解決するための手段】上記課題を達成するために、本発明に係る暗号通信システムは、暗号通信装置と、自端末装置を識別可能な所定ビット数のビット列なる端末識別子を、当該暗号通信装置に送信する機能を有する複数の端末装置と、無効化すべき端末装置を特定するものとして1以上の端末識別子を示す無効化端末特定情報を生成する管理装置とを備える暗号通信システムであって、前記管理装置は、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを有し、前記暗号通信装置は、前記管理装置により出力された前記無効化端末特定情報を取得する無効化端末特定情報取得手段と、端末装置から端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、一方、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを有することを特徴とする。

【0015】ここで、暗号通信装置は、例えば実施の形態1〜3で示すようなコンテンツ鍵配信装置であり、所定の通信とは例えば暗号化コンテンツ鍵の送信であり、無効化端末特定情報は例えば実施の形態1〜3において示すTRLである。本発明により、あるビット列を含む全ての端末IDを、それに含まれる共通するビット列の値と位置とを特定する情報で包括的に表現するので、TRLのデータ量を比較的小さく抑えることができるようになり、この結果、一部の無効化すべき端末装置を除い

た適切な端末装置に対してのみ、コンテンツ鍵を暗号化して配信する等の暗号通信に係るサービスを行う実用的な暗号通信システムが実現される。

【0016】また、本発明に係る管理装置は、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき1以上の各端末装置の各端末識別子を示す無効化端末特定情報を生成する管理装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを備えることを特徴とする。

【0017】また、本発明に係る暗号通信装置は、複数の端末装置のうち自端末装置を識別可能な所定ビット数のビット列なる端末識別子を保持する各端末装置との間で通信を行う暗号通信装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて構成され、無効化すべき端末装置を特定するためのものとして1以上の各端末装置の各端末識別子を示した無効化端末特定情報を外部から取得する無効化端末特定情報取得手段と、端末装置から、当該端末装置が保持する端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを備えることを特徴とする。

【0018】また、本発明に係る情報生成方法は、複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成方法であって、前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップとを含むことを特徴とする。

【0019】

【発明の実施の形態】以下、本発明をコンテンツの著作権保護等に配慮したシステムに応用した一実施形態であるコンテンツ鍵配信システムについて、図面を用いて説明する。

<実施の形態1>

<システム構成>図1は、本発明の実施の形態1に係るコンテンツ鍵配信システムの構成図である。

【0020】コンテンツ鍵配信システム100は、コンテンツを再生する複数のコンテンツ再生装置130と、暗号化されたコンテンツ鍵（以下、「暗号化コンテンツ鍵」という。）を各コンテンツ再生装置の要求に応じて配信するコンテンツ鍵配信装置120と、コンテンツ鍵配信装置120に対して暗号化コンテンツ鍵の配信可否の判断材料となる情報である無効化端末リスト（TRL）を送信する管理装置110を含んで構成される。なお、コンテンツ鍵配信システム100においてコンテンツ鍵配信装置120は、1台又は複数台備えられる。

【0021】ここで、コンテンツ再生装置130a、130b等は、例えば各家屋に設置され、通信路又は記録媒体等を経由して暗号化されたコンテンツを取得し、そのコンテンツをコンテンツ鍵を用いて復号して再生する機能を有する装置である。著作権保護等に配慮したシステムにおいては、コンテンツは暗号化され流通の対象とされることを想定している。このため、コンテンツ再生装置は、暗号化コンテンツ鍵をコンテンツ鍵配信装置120から受信し復号することによりコンテンツ鍵を得なければ、その暗号化されたコンテンツを、復号できず、そのため再生できない。

【0022】コンテンツ再生装置130（以下、「端末」ともいう。）は各々、CPU、メモリ、ハードディスク、外部との通信機構等を備えておりディスプレイ装置やスピーカ等を通じて、映画等のコンテンツをユーザに視聴可能なように再生するコンテンツ再生処理を行う装置であって、機能的には端末ID記憶部131、復号鍵記憶部132、暗号化コンテンツ格納部133、要求送出部134、暗号化コンテンツ鍵受信部135、復号部136及び再生部137を有する。

【0023】端末ID記憶部131は、各端末を識別するための端末IDを記憶しているROM（read only memory）等の一記憶領域である。例えば、コンテンツ鍵配信システム100において16台の端末が用いられ得る場合には、16台を識別可能な4ビット以上のビット列で端末IDは構成され、例えば、50億台の端末を想定する場合には端末IDは32ビットを超えるビット列となる。なお、実施の形態1においては、説明の便宜上、16台の端末を想定して、端末IDを4ビットとした例を主に用いて説明する。

【0024】復号鍵記憶部132は、暗号化コンテンツ鍵の復号用に用いられる復号鍵を記憶しているROM等

の一記憶領域である。この復号鍵は、端末毎に固有の値を有する秘密鍵であり、例えば128ビットで構成される。暗号化コンテンツ格納部133は、暗号化されたコンテンツを格納するハードディスク等の記録媒体の一領域である。なお、端末は暗号化されたコンテンツを受信等により外部から取得して暗号化コンテンツ格納部133に格納する機能を有する。

【0025】要求送出部134は、端末ID記憶部131に記憶されている端末IDを含む送信要求情報を公衆網等の通信路101を通じてコンテンツ鍵配信装置120に送信する機能を有する。暗号化コンテンツ鍵受信部135は、コンテンツ鍵配信装置120から暗号化コンテンツ鍵が送信された場合にその暗号化コンテンツ鍵を受信する機能を有する。

【0026】復号部136は、暗号化コンテンツ鍵受信部135により受信された暗号化コンテンツ鍵を受け取ると復号鍵記憶部132に記憶されている復号鍵を用いてその暗号化コンテンツ鍵を復号し、復号の結果として得られるコンテンツ鍵を再生部137に送出する機能を有する。また、再生部137は、暗号化コンテンツ格納部133に格納されている暗号化されているコンテンツを、復号部136から伝えられたコンテンツ鍵を用いて復号して再生する機能を有する。この再生部137によりコンテンツが再生されると、ユーザはコンテンツを視聴できる。

【0027】なお、要求送出部134、暗号化コンテンツ鍵受信部135、復号部136及び再生部137の行う機能の一部は、メモリに格納された制御プログラムがCPUに実行されることにより実現される。管理装置110は、例えばコンテンツの著作権等の保護に関する業務を行う機関に設置されるコンピュータ等であり、各端末130のうち、内部に記憶されている復号鍵が暴露される等により著作権等の保護が図れない事態に陥っている全ての端末、即ち暗号化コンテンツ鍵の配信先にすべきでない全ての端末を、特定するための情報を主たる内容とするTRLを生成してコンテンツ鍵配信装置120に送信するTRL生成送信処理を行う装置である。以下、暗号化コンテンツ鍵の配信先にすべきでない端末を無効化端末という。

【0028】この管理装置110は、図1に示すように、無効化端末ID群取得部111、TRL生成部112、TRL送信部113を備える。ここで、無効化端末ID群取得部111は、全ての無効化端末についての端末IDを特定する情報を取得し、取得した各端末IDをTRL生成部112に与える機能を有する。

【0029】TRL生成部112は、無効化端末ID群取得部111から与えられた各端末IDに基づいて無効化端末を特定する情報を主たる内容とするTRLを生成し、TRL送信部113に伝える機能を有する。なお、このTRLの生成については、後に詳しく説明する。ま

た、TRL送信部113は、TRL生成部112から伝えられたTRLを通信路を通じてコンテンツ鍵配信装置120に対して送信する機能を有する。

【0030】管理装置110が行うTRL生成送信処理の手順については後に説明する。なお、この管理装置110は、定期的或いはTRLに含めるべき無効化端末の情報が変化した時等に、TRLをコンテンツ鍵配信装置120に送信するように運用されることが想定される。コンテンツ鍵配信装置120は、各端末からの暗号化コンテンツ鍵の送信要求を受けるとその端末が無効化端末でない場合に限りその端末に暗号化コンテンツ鍵を送信することを内容とするコンテンツ鍵配信処理を行うコンピュータであり、機能的には、TRL格納部121、TRL受信部122、コンテンツ鍵記憶部123、暗号化鍵群記憶部124、送信要求受付部125、照合部126、暗号化部127及び暗号化コンテンツ鍵送信部128を有する。

【0031】ここで、TRL格納部121は、TRLを格納するためのハードディスク等の記録媒体の一領域である。TRL受信部122は、管理装置110から送信されるTRLを受信してTRL格納部121に格納する機能を有する。コンテンツ鍵記憶部123は、コンテンツ鍵を記憶しているメモリ等の一記憶領域である。

【0032】暗号化鍵群記憶部124は、各端末について、その復号鍵に呼応する暗号化鍵とその端末の端末IDと対応付けて、予め格納しているハードディスク等の一領域である。送信要求受付部125は、公衆網等を通じて各端末から送られる送信要求を受け付けて、送信要求に含まれる端末IDを照合部126に伝える機能を有する。

【0033】照合部126は、送信要求受付部125から伝えられた端末IDが、TRLにより特定される無効化端末のいずれかと一致するか否かを照合することにより送信要求元の端末が無効化端末であるか否かを判定し、無効化端末であると判定した場合にはエラーメッセージを送信元に返すべき旨の指示を暗号化コンテンツ鍵送信部128に伝え、無効化端末でないと判定した場合には送信要求受付部125から伝えられた端末IDを暗号化部127に伝える機能を有する。

【0034】暗号化部127は、照合部126から端末IDを伝えられた場合には、暗号化鍵群記憶部124においてその端末IDと対応付けられている暗号化鍵を用いて、コンテンツ鍵記憶部123に格納されているコンテンツ鍵を暗号化することにより、暗号化コンテンツ鍵を生成して暗号化コンテンツ鍵送信部128に送出する機能を有する。

【0035】また、暗号化コンテンツ鍵送信部128は、照合部126からエラーメッセージを送信元に返すべき旨の指示を伝えられた場合には、送信要求を発した端末に対してエラーメッセージを送信し、暗号化部12

7から暗号化コンテンツ鍵を伝えられた場合には、送信要求を発した端末に対してその暗号化コンテンツ鍵を送信する機能を有する。

【0036】<端末ID／復号鍵／暗号化鍵>図2は、各端末が記憶している端末IDと復号鍵とを示す図である。コンテンツ鍵配信システム100が、16台の端末を含み、端末IDは4ビットである場合において、同図に示すように、例えば端末0は「0000」という端末IDと復号鍵DK0を保持し、端末1は「0001」という端末IDと復号鍵DK1を保持し、端末15は「1111」という端末IDと復号鍵DK15を保持している。なお、復号鍵DK0、DK1、・・・、DK15はいずれも、相互に値が一致しないビット列である。また、各端末は、復号鍵を耐タンパ技術等によって秘密状態で保護する。

【0037】図3は、各端末が保持する端末IDの値の決定方法を示す概念図である。例えば著作権等の保護に関する業務を行う機関によって、各メーカーの製造する各端末への端末IDの割り当てが定められ、メーカーは端末の製造段階において、その割り当てに従って各端末にその割り当てられた端末IDを記憶したROM等をセ

ットする。

【0038】図3中の円をノードといい、円と円を繋ぐ直線をバスと表現すると、図3では、16台の各端末を最下位レイヤの各々のノード12と対応付けるように2分木の木構造を定め、あるノードから下位のレイヤのノードへの2つのバスそれぞれに「0」と「1」とのいずれかの値を付している。各端末の端末IDは、最上位レイヤのノード11からその端末に対応する最下位レイヤのノード12とを結ぶ全てのバスに付された「0」又は「1」の値を、上位のレイヤから下位のレイヤの方向に連結して得られたビット列で表される。従って、図2で示したように各端末について端末IDが定められる。

【0039】図4は、コンテンツ鍵配信装置120の暗号化鍵群記憶部124に記憶されるデータの内容例を示した図である。暗号化鍵群記憶部124には、同図に示すように、全ての端末に対する端末IDと暗号化鍵とが対応付けられて格納されている。例えば、「0000」という端末IDには暗号化鍵EK0が対応付けられており、この暗号化鍵EK0は端末0に保持されている復号鍵DK0と呼応する鍵である。従って、暗号化鍵EK0を用いて暗号化されたデータは復号鍵DK0を用いて復号することが可能となる。

【0040】なお、暗号化鍵EK<sub>i</sub>とそれに対応する復号鍵DK<sub>i</sub>は、コンテンツ鍵を暗号化するための暗号化アルゴリズムに秘密鍵暗号系を用いるのであればEK<sub>i</sub>とDK<sub>i</sub>とは一致し、公開鍵暗号系を用いるのであればEK<sub>i</sub>とDK<sub>i</sub>とは一致はしないが対となるものである。

<システム動作>以下、コンテンツ鍵配信システム10

0のシステム動作の概要について説明する。

【0041】<管理装置の動作>図5は、管理装置110が行うTRL生成送信処理を示すフローチャートである。管理装置110のTRL生成部112は、無効化端末ID群取得部111より無効化端末についての端末ID群を取得し(ステップS21)、TRLにおける無効化端末を特定する情報部分(以下、「端末ID関連情報」という。)の内容を算定するTRL用データ生成処理を行う(ステップS22)。TRL用データ生成処理の詳細については後述する。

【0042】TRL用データ生成処理の後、TRL生成部112は、生成した端末ID関連情報を含めたTRLを構築し(ステップS23)、そのTRLをTRL送信部113に伝え、これを受けてTRL送信部113はそのTRLを通信路を通じてコンテンツ鍵配信装置120に送信する(ステップS24)。

<コンテンツ再生装置の動作>図6は、コンテンツ再生装置130が行うコンテンツ再生処理を示すフローチャートである。

【0043】コンテンツ再生装置130(端末)は、例えばユーザのコンテンツ再生を指示する操作を受けたとき等に、コンテンツ再生処理を行う。まず、端末の要求送出部134が、端末ID記憶部131に記憶されている自端末固有の端末IDを含めたデータで構成される送信要求を通信路を通じてコンテンツ鍵配信装置120に送信することにより、暗号化コンテンツ鍵の送信を要求する(ステップS31)。なお、この送信要求に応答して、コンテンツ鍵配信装置120からは暗号化コンテンツ鍵、又はエラーメッセージが送られることになる。

【0044】送信要求の後に、暗号化コンテンツ鍵受信部135は、暗号化コンテンツ鍵の受信に成功したかを判定し(ステップS32)、暗号化コンテンツ鍵が正常に受信された場合に限り、その暗号化コンテンツ鍵を復号部136に伝える。これを受けて復号部136は復号鍵記憶部132に保持されている復号鍵を用いて暗号化コンテンツ鍵を復号して、その復号の結果として得られるコンテンツ鍵を再生部137に伝える(ステップS33)。

【0045】コンテンツ鍵を伝えられると再生部137は、暗号化コンテンツ格納部133に格納されている暗号化されたコンテンツをそのコンテンツ鍵を用いて復号しつつ再生する(ステップS34)。この再生により、例えばディスプレイ装置やスピーカを通じて映像、音声等が出力され、ユーザはコンテンツの視聴が可能になる。

【0046】<コンテンツ鍵配信装置の動作>図7は、コンテンツ鍵配信装置120が行うコンテンツ鍵配信処理を示すフローチャートである。コンテンツ鍵配信装置120は、TRLを、コンテンツ鍵配信処理を行う前に少なくとも1度はTRL受信部122により受信してT



RL 格納部 121 に格納しており、コンテンツ再生装置 130 から送信要求が送られる度にコンテンツ鍵配信処理を行う。

【0047】コンテンツ再生装置 130 (端末) から送信要求が送られると、送信要求受付部 125 は送信要求を受信しその送信要求に含まれる端末 ID を照合部 126 に伝える (ステップ S41)。照合部 126 は、端末 ID が伝えられると、TRL を参照してその端末 ID が無効化端末の端末 ID であるか否かを判定する TRL 照合処理を行う (ステップ S42)。なお、TRL 照合処理の詳細については後述する。

【0048】TRL 照合処理の結果として、送信要求に係る端末 ID が、無効化端末の端末 ID であると判定した場合には (ステップ S43)、照合部 126 はエラーメッセージを送信要求の送信元の端末に返すべき旨の指示を暗号化コンテンツ鍵送信部 128 に伝えて、これに応じて暗号化コンテンツ鍵送信部 128 がエラーメッセージをその端末に送信するといったエラー処理を行い (ステップ S47)、コンテンツ鍵配信処理を終了する。

【0049】ステップ S43 において TRL 照合処理の結果として、送信要求に係る端末 ID が、無効化端末の端末 ID ではないと判定した場合には、照合部 126 は、送信要求に係る端末 ID を暗号化部 127 に伝え、これを受けて暗号化部 127 は、その端末 ID に対応する暗号化鍵を暗号化鍵群記憶部 124 から取り出してその暗号化鍵を用いて、コンテンツ鍵記憶部 123 に記憶されているコンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、その暗号化コンテンツ鍵を暗号化コンテンツ鍵送信部 128 に伝える (ステップ S45)。

【0050】暗号化コンテンツ鍵を伝えられると、暗号化コンテンツ鍵送信部 128 はその暗号化コンテンツ鍵を送信要求を発した端末に送信し (ステップ S46)、これでコンテンツ鍵配信処理は終了する。

<TRL の構成> 図 8 は、実施の形態 1 における TRL のデータ構成を示す図である。

【0051】なお、同図中のビットサイズ例は端末が 16 台の場合を想定しているが、括弧内には、参考のため実用的な例として、端末数が数億台以上である場合に対応したビットサイズの例を示している。以下、端末が 16 台の場合についてのビットサイズ例を用いて説明する。同図に示すように、TRL は、8 ビットのバージョン情報 210 と、端末 ID 関連情報 220 と、64 ビットの署名情報 230 とから構成される。

【0052】バージョン情報 210 は、TRL のバージョン番号を示す情報であり、例えば内容の異なる TRL が新たに生成される毎に、そのバージョン番号が変えられる。端末 ID 関連情報 220 は、グループ情報 221 と個別情報 225 とから構成される。

【0053】グループ情報 221 は、ID223 とマ

クデータ 224 との組の 1 個又は複数個を含み、その個数を示すエントリ数 222 を含む。その組の数が M 個であれば、エントリ数 222 の示す値は M となる。ここで、マスクデータ 224 は、これを構成する 4 ビットのビット列のうち上位 X ビットを「1」にし残りの下位ビットがあればその下位ビット全てを「0」とした形式のデータであり、これにより X が表現される。

【0054】また、X を表すマスクデータ 224 と組をなす ID223 は、これを構成する 4 ビットのビット列のうち上位から X ビット分の内容のみが有用であり、その他の値は例えば「0」とした形式のデータとなる。この ID223 とマスクデータ 224 との組により、マスクデータ 224 で表される上位 X ビットが ID223 の値と一致する全ての端末 ID を、即ち 2 の (4-X) 乗個の無効化端末の端末 ID を示す。

【0055】従って、グループ情報 221 は、複数の無効化端末の端末 ID を包括的に表現する 1 又は複数の組から成る。個別情報 225 は、1 又は複数個の ID227 を含む、その個数を示すエントリ数 226 を含む。ID227 の個数が N 個であれば、エントリ数 226 の示す値は N となる。

【0056】この ID227 は、無効化端末の端末 ID を示す。従って、個別情報 225 は、個別に無効化端末の端末 ID を表現する 1 又は複数の情報から成る。署名情報 230 は、バージョン情報 210 及び端末 ID 関連情報 220 の全体を反映して作成されるいわゆるデジタル署名である。図 9 は、TRL の内容例を示す図である。

【0057】同図では、グループ情報として、ID223 がビット列「1100」であってマスクデータ 224 がビット列「1100」である組と ID223 がビット列「0110」であってマスクデータ 224 がビット列「1110」である組とを有し、個別情報として、ID227 がビット列「0001」である情報を含む TRL を例示している。

【0058】この「1100」なるマスクデータと「1100」なる ID との組により、「1100」、「1101」、「1110」及び「1111」という 4 個の無効化端末の端末 ID が表され、また、「1110」なるマスクデータと「0110」なる ID との組により、「0110」及び「0111」という 2 個の無効化端末の端末 ID が表される。

【0059】従って、図 9 に示す TRL は、グループ情報で 6 個と個別情報で 1 個の合計 7 個の無効化端末の端末 ID を示している。

<TRL 用データ生成処理> 図 10 は、実施の形態 1 における管理装置 110 により行われる TRL 生成送信処理の一部である TRL 用データ生成処理を示すフローチャートである。なお、同図では、端末 ID を N ビットと汎用的に表現しているが、ここでは 4 ビットであるもの



として説明する。

【0060】管理装置110においてTRL生成部112は、無効化端末ID群取得部111より無効化端末についての端末ID群を取得した後にTRL用データ生成処理を行う(図5参照)。まず、TRL生成部112は、取得した端末ID群をメモリ等の記憶媒体の一領域である作業用ID領域に格納し(ステップS201)、メモリ等の記憶媒体の一領域である作業用ビット領域に1ビットのビットデータ「0」と「1」との2つを格納し(ステップS202)、変数Xに1を設定する(ステップS203)。

【0061】続いて、TRL生成部112は、作業用ビット領域中、未着目のXビットのビットデータの1つに着目し(ステップS204)、作業用ID領域中に格納されている端末IDのうち、上位Xビットが着目中のビットデータと一致するという条件を満たすものの数をカウントする(ステップS205)。ステップS205の結果、カウント数が2の(4-X)乗となった場合には(ステップS206)、TRL生成部112は、ステップS205におけるその条件を満たす端末IDを作業用ID領域から削除し(ステップS207)、その条件を満たす端末IDについて、上位Xビット分を「1」として他のビットを「0」とした4ビットのビット列をマスクデータとして、更に上位Xビット分を着目中のビットデータと同一にして他のビットを「0」とした4ビットのビット列をIDとして、そのマスクデータとIDとを対応付けてグループ情報としてメモリ等の記憶媒体の一領域に保存し(ステップS208)、ステップS209の判断を行う。

【0062】また、ステップS205の結果、カウント数が0又は1であった場合には(ステップS206)、TRL生成部112は、ステップS207及びステップS208をスキップしてステップS209の判断を行う。また、ステップS205の結果、カウント数が2の(4-X)乗、0及び1のいずれでもない場合には(ステップS206)、TRL生成部112は、ステップS205におけるその条件を満たす端末IDのうち上位からX+1ビット目が「0」のものが2個以上存在すれば、着目中のビットデータの低位に1ビットの「0」を加えて形成されるビットデータを作業用ビット領域に格納し(ステップS210)、その条件を満たす端末IDのうち上位からX+1ビット目が「1」のものが2個以上存在すれば、着目中のビットデータの低位に1ビットの「1」を加えて形成されるビットデータを作業用ビット領域に格納し(ステップS211)、ステップS209の判断を行う。

【0063】ステップS209では、TRL生成部112は、未着目のXビットのビットデータが存在するか否かを判定し、未着目のXビットのビットデータが未だ存在すればステップS204に戻って次のビットデータに

着目して処理を行い、未着目のXビットのビットデータが存在しなければ変数Xを1増加し(ステップS212)、変数Xが4と等しいか否かを判定する(ステップS213)。

【0064】TRL生成部112は、ステップS213において変数Xが4と等しくないと判定した場合には、再びステップS204に戻って次のビットデータに着目して処理を行い、変数Xが4と等しいと判定した場合には、作業用ID領域に端末IDが残っていればその全ての端末IDを個別情報中のIDとしてメモリ等の記憶媒体の一領域に保存し(ステップS214)、これによりTRL用データ生成処理を終了する。

【0065】なお、図5のステップS23で示すTRLの構築は、上述のTRL用データ生成処理によって記憶媒体の一領域に保存されたグループ情報及び個別情報に、それぞれエントリ数を付加して、更にバージョン情報及び署名情報を加えることによって実行される。従って、例えば、TRL生成部112が無効化端末ID群取得部111から「0001」、「0110」、「0111」、「1100」、「1101」、「1110」及び「1111」の7個の端末IDを取得した場合には、上述の手順により、図9に例示した内容のTRLが生成されることになる。このTRLは、図3において隣接した端末6及び端末7のグループと、端末12～端末15のグループと、更に端末1が無効化端末であることを表している。

【0066】また、無効化端末が1台もない場合には、TRLのグループ情報中のエントリ数は0となり、個別情報中のエントリ数も0となる。

<TRL照合処理>図11は、実施の形態1におけるコンテンツ鍵配信装置120により行われるコンテンツ鍵配信処理の一部であるTRL照合処理を示すフローチャートである。

【0067】コンテンツ鍵配信装置120の照合部126は、端末から送られた端末IDを送信要求受付部125より得る度にこのTRL照合処理を行う。照合部126は、端末から送られた端末IDと一致するID227が、TRL格納部121に格納されているTRL中の個別情報225中に存在するか否かを判定し(ステップS221)、一致するID227が存在すれば端末から取得した端末IDは無効化端末の端末IDであると判定し(ステップS222)、TRL照合処理を終了する。

【0068】ステップS221において、端末から送られた端末IDと一致するID227がTRLの個別情報225中に含まれていないと判定した場合には、照合部126は、TRLのグループ情報中の1組のID223及びマスクデータ224で表されるいずれかの端末IDと、端末から送られた端末IDとが一致するかを検査する(ステップS223、S224)。

【0069】即ち、照合部126は、端末から送られた

端末IDとマスクデータ224とのビット毎の論理積を求めて(ステップS223)、求めた論理積がそのマスクデータ224と組をなすID223と一致するか否かを判定し(ステップS224)、一致すれば、端末から取得した端末IDは無効化端末の端末IDであると判定し(ステップS222)、TRL照合処理を終了する。

【0070】また、ステップS224において、一致しない場合には、照合部126はTRLのグループ情報中の全てのID223とマスクデータ224との組についてステップS223及びステップS224の処理を行なったかを判定し(ステップS225)、全ての組についての処理済みでない場合にはステップS223及びステップS224の処理を再び行う。

【0071】ステップS225において、全ての組について処理済みであると判定した場合には、照合部126は、端末から取得した端末IDは無効化端末の端末IDでないと判定し(ステップS226)、TRL照合処理を終了する。以下、TRL格納部121に格納されているTRLは図9に例示した内容であることを前提として、図7及び図11を用いて、端末13から端末ID「1101」を含めた送信要求がコンテンツ鍵配信装置120に送られた場合を想定してコンテンツ鍵配信装置120の具体的な動作について説明する。

【0072】コンテンツ鍵配信装置120の送信要求受付部125は、端末13から送られた端末ID「1101」を取得して照合部126に伝え(ステップS41)、照合部126は、端末13から送られた端末ID「1101」がTRLの個別情報中にあるか否かを判定する(ステップS221)、個別情報中には「0001」というIDしか含まれていないため、端末ID「1101」とグループ情報中のマスクデータ「1100」との論理積を求める(ステップS223)。

【0073】このステップS223により求められる論理積は「1100」となり、照合部126は、その求められたビット列「1100」とID「1100」とが一致するか否かを判定し(ステップS224)、一致するので、端末から取得した端末IDは無効化端末のIDであると判定し(ステップS222)、この結果(ステップS43)、エラーメッセージを送信すべき旨を暗号化コンテンツ鍵送信部128に伝え、これを受けて暗号化コンテンツ鍵送信部128がエラーメッセージを端末13に送信する(ステップS47)。

【0074】次に、同じ前提の下で、復号鍵DK2を保持する端末2から端末ID「0010」を含めた送信要求がコンテンツ鍵配信装置120に送られた場合を想定してコンテンツ鍵配信装置120の具体的な動作について説明する。コンテンツ鍵配信装置120の送信要求受付部125は、端末2から送られた端末ID「0010」を取得して照合部126に伝え(ステップS41)、照合部126は、端末2から送られた端末ID「0010」がTRLの個別情報中にあるか否かを判定する(ステップS221)、個別情報中には「0001」というIDしか含まれていないため、端末ID「0010」とグループ情報中のマスクデータ「1100」との論理積を求める(ステップS223)。

【0075】こうして求められる論理積は「0000」となり、照合部126は、その求められたビット列「0000」とID「1100」とが一致するか否かを判定し(ステップS224)、一致しないので、次に、端末から送られた端末ID「0010」と、グループ情報中のマスクデータ「1110」との論理積を求める(ステップS225、ステップS223)。

【0076】こうして求められる論理積は「0010」となり、照合部126は、その求められたビット列「0010」とID「0110」とが一致するか否かを判定し(ステップS224)、一致せず、未処理のグループ情報中のマスクデータは既にないため(ステップS225)、端末から取得した端末ID「0010」は無効化端末の端末IDでないと判定し(ステップS226、S43)、その端末ID「0010」を暗号化部127に伝える。

【0077】これを受けて暗号化部127は、暗号化鍵群記憶部124から「0010」に対応する暗号化鍵EK2(図4参照)を抽出して用いることにより、コンテンツ鍵記憶部123に格納されているコンテンツ鍵を暗号化して(ステップS45)、その結果として得られる暗号化コンテンツ鍵を暗号化コンテンツ鍵送信部128に伝える。

【0078】暗号化コンテンツ鍵を伝えられると暗号化コンテンツ鍵送信部128は、その暗号化コンテンツ鍵を端末2に送信する(ステップS46)。従って、この暗号化コンテンツ鍵を取得した端末2は、内部に保持する復号鍵DK2を用いて復号し、コンテンツ鍵を得ることができる。

＜実施の形態2＞以下、実施の形態2に係るコンテンツ鍵配信システムについて説明する。

【0079】この実施の形態2に係るコンテンツ鍵配信システムは、実施の形態1で示したコンテンツ鍵配信システム100と基本的に同様のシステム構成を有し、基本的に同様のシステム動作を行う。従って、各装置については図1等で付した符号を用いて示し、また、実施の形態1と同等の部分についての説明は省略する。但し、実施の形態2では、端末IDのデータ構成を特別なものと定めており、また、TRLのデータ構造を実施の形態1におけるものとは異なったものになっている。このため、管理装置110は実施の形態1で示したTRL用データ生成処理とは異なるTRL用データ生成処理を行い、コンテンツ鍵配信装置120は実施の形態1で示したTRL照合処理とは異なるTRL照合処理を行う。

【0080】＜端末ID＞図12は、実施の形態2にお

ける端末IDのデータ構成を示す図である。同図では、コンテンツ鍵配信システムにおける端末数として数億台以上に対応できるように端末IDを128ビットのものとした構成例を示している。端末IDは、32ビットのメーカーIDフィールド301、32ビットの製品IDフィールド302、32ビットの製品バージョンIDフィールド303、及び32ビットのシリアル番号フィールド304で構成される。

【0081】ここで、メーカーIDフィールド301には、コンテンツ再生装置を製造する各メーカーを識別するためのメーカーIDが格納される。製品IDフィールド302には、メーカーIDで定まるメーカーにおける各製品を識別するための製品IDが格納される。製品バージョンIDフィールド303には、製品IDで定まる製品について形式変更等の都度変更されるバージョン番号等を示す製品バージョンIDが格納される。

【0082】また、シリアル番号フィールド304には、製品個別に付されるシリアル番号が格納される。

<TRLの構成>図13は、実施の形態2におけるTRLのデータ構成を示す図である。同図では、端末数が数億台以上である場合に対応したTRLのデータ構成例を示している。

【0083】同図に示すように、TRLは、8ビットのバージョン情報310と、128ビットの発行者情報320と、128ビットの無効化端末数330と、端末ID関連情報340と、320ビットの署名情報350とから構成される。バージョン情報310は、TRLのバージョン番号を示す情報であり、例えば内容の異なるTRLが新たに生成される毎に、そのバージョン番号が変えられる。

【0084】発行者情報320は、管理装置等、TRLの発行元を示す情報である。無効化端末数330は、無効化端末の端末数である。端末ID関連情報340は、128ビットのID342と8ビットのマスク用ビット343との組の1個又は複数個を含み、その個数を示すエントリ数341を含む。その組の数がN個であれば、エントリ数341の示す値はNとなる。

【0085】ここで、マスク用ビット343は、1~128の値をとる。なお、このマスク用ビット343の値をXとすると、128ビットのビット列のうち上位Xビットを「1」にし残りの下位ビットがあればその下位ビット全てを「0」とした形式のマスクデータを導出することができる。また、マスク用ビット343と組をなすID342は、これを構成する128ビットのビット列のうち上位からマスク用ビット343で示される値のビット桁数分の内容のみが有用であり、その他の値は例えば「0」とした形式のデータとなる。

【0086】このID342とマスク用ビット343との組により、マスク用ビット343の値Xで表される上位XビットがID342の値と一致する全ての端末ID

を、即ち2の(128-X)乗個の無効化端末の端末IDを示す。署名情報350は、バージョン情報310、発行者情報320、無効化端末数330及び端末ID関連情報340の全体を反映して作成されるいわゆるデジタル署名である。

【0087】<TRL用データ生成処理>図14は、実施の形態2における管理装置110により行われるTRL生成送信処理の一部であるTRL用データ生成処理を示すフローチャートである。ここでは、端末IDをNビットであるとして説明する。Nは、例えば128ビットである。

【0088】管理装置110においてTRL生成部112は、無効化端末ID群取得部111より無効化端末についての端末ID群を取得した後にTRL用データ生成処理を行う(図5参照)。まず、TRL生成部112は、取得した端末ID群をメモリ等の記憶媒体の一領域である作業用ID領域に格納し(ステップS301)、メモリ等の記憶媒体の一領域である作業用ビット領域に1ビットのビットデータ「0」と「1」との2つを格納し(ステップS302)、変数Xに1を設定する(ステップS303)。

【0089】続いて、TRL生成部112は、作業用ビット領域中、未着目のXビットのビットデータの1つに着目し(ステップS304)、作業用ID領域中に格納されている端末IDのうち、上位Xビットが着目中のビットデータと一致するという条件を満たすものの数をカウントする(ステップS305)。ステップS305の結果、カウント数が2の(N-X)乗となった場合には(ステップS306)、TRL生成部112は、ステップS305におけるその条件を満たす端末IDを作業用ID領域から削除し(ステップS307)、その条件を満たす端末IDについて、変数Xの値をマスク用ビットとして、更に上位Xビット分を着目中のビットデータと同一にして他のビットを「0」としたNビットのビット列をIDとして、そのマスク用ビットとIDとを一組としてメモリ等の記憶媒体の一領域に保存し(ステップS308)、ステップS309の判断を行う。

【0090】また、ステップS305の結果、カウント数が0又は1であった場合には(ステップS306)、TRL生成部112は、ステップS307及びステップS308をスキップしてステップS309の判断を行う。また、ステップS305の結果、カウント数が2の(N-X)乗、0及び1のいずれでもない場合には(ステップS306)、TRL生成部112は、ステップS305におけるその条件を満たす端末IDのうち上位からX+1ビット目が「0」のものが2個以上存在すれば、着目中のビットデータの下位に1ビットの「0」を加えて形成されるビットデータを作業用ビット領域に格納し(ステップS310)、その条件を満たす端末IDのうち上位からX+1ビット目が「1」のものが2個以

上存在すれば、着目中のビットデータの下位に1ビットの「1」を加えて形成されるビットデータを作業用ビット領域に格納し（ステップS311）、ステップS309の判断を行う。

【0091】ステップS309では、TRL生成部112は、未着目のXビットのビットデータが存在するか否かを判定し、未着目のXビットのビットデータが未だ存在すればステップS304に戻って次のビットデータに着目して処理を行い、未着目のXビットのビットデータが存在しなければ変数Xを1増加し（ステップS312）、変数XがNと等しいか否かを判定する（ステップS313）。

【0092】TRL生成部112は、ステップS313において変数XがNと等しくないとき判定した場合には、再びステップS304に戻って次のビットデータに着目して処理を行い、変数XがNと等しいとき判定した場合には、作業用ID領域に端末IDが残っていればその全ての端末IDについて、Nをマスク用ビットとしてその端末IDをIDとして一組とし、メモリ等の記憶媒体の一領域に保存し（ステップS314）、これによりTRL用データ生成処理を終了する。

【0093】なお、実施の形態2においては、図5のステップS23で示すTRLの構築は、上述のTRL用データ生成処理によって記憶媒体の一領域に保存されたIDとマスク用ビットとの1個又は複数個の組にエントリ数を付加し、更にバージョン、発行者情報、無効化端末数及び署名情報を加えることによって実行される。図15は、TRLの内容例を示す図である。

【0094】同図では、項目としては図13に示したデータ項目を有し、端末IDを4ビットのビット列とし、マスク用ビットは1～4までを表す2ビットのデータであることとしたTRLの内容例を示している。なお、この図15に例示する端末ID関連情報が表現する全ての無効化端末の端末IDは、図9に例示する端末ID関連情報が表現する全ての無効化端末の端末IDと同じである。

【0095】＜TRL照合処理＞図16は、実施の形態2におけるコンテンツ鍵配信装置120により行われるコンテンツ鍵配信処理の一部であるTRL照合処理を示すフローチャートである。コンテンツ鍵配信装置120の照合部126は、端末から送られた端末IDを送信要求受付部125より得る度にこのTRL照合処理を行う。

【0096】照合部126は、端末から送られた端末IDと、TRLの端末ID関連情報中のIDとマスク用ビットとの組のいずれかで表される端末IDとが一致するかを検査する（ステップS321～S324）。即ち、照合部126は、TRL中の1つの未着目のマスク用ビットに着目し、そのマスク用ビットの値に応じたマスクデータを上述したように導出して（ステップS32

1）、端末から送られた端末IDと、導出したマスクデータとのビット毎の論理積を求めて（ステップS322）、求めた論理積が着目中のマスク用ビット343と組をなすID342と一致するか否かを判定し（ステップS323）、一致すれば、端末から取得した端末IDは無効化端末の端末IDであると判定し（ステップS326）、TRL照合処理を終了する。

【0097】また、ステップS323において、一致しない場合には、照合部126はTRL中の全てのマスク用ビット343に着目してステップS321～S323の処理を行なったかを判定し（ステップS324）、全てのマスク用ビット343に着目して処理を行っていない場合にはステップS321に戻って未着目のマスク用ビットに着目して処理を行う。

【0098】ステップS324において、全てのマスク用ビットについて処理済みであると判定した場合には、照合部126は、端末から取得した端末IDは無効化端末の端末IDでないと判定し（ステップS325）、TRL照合処理を終了する。

20 <考察>実施の形態2に示したコンテンツ鍵配信システムにおいては、端末IDが図12に示したようなデータ構造であるため、あるメーカーが製造した特定バージョンの製品に実装されたあらゆるコンテンツ再生装置が無効化すべきものとなったような場合において、装置内に保持する端末IDのシリアル番号フィールドの内容のみが異なる一群のコンテンツ再生装置の全てを、少ないデータ量で特定するTRLを管理装置は生成してコンテンツ鍵配信装置に送信することができるようになる。

【0099】そのTRLは、例えば、マスク用ビット343の値を96とし、ID342をそのメーカーのその製品のそのバージョンを特定し、かつ、シリアル番号については0としたビット列とした一組のみを端末ID関連情報として含むものとなる。

<実施の形態3>以下、実施の形態3に係るコンテンツ鍵配信システムについて説明する。

【0100】この実施の形態3に係るコンテンツ鍵配信システムは、実施の形態1で示したコンテンツ鍵配信システム100と基本的に同様のシステム構成を有し、基本的に同様のシステム動作を行う。従って、各装置については図1等で付した符号を用いて示し、また、実施の形態1と同等の部分についての説明は省略する。但し、実施の形態3では、端末IDのデータ構造は実施の形態2で示したものを採用し、またTRLのデータ構造を、実施の形態1におけるものとは異なり、実施の形態2におけるTRLに若干のデータ項目を追加したものとしている。このため、管理装置110は実施の形態2で示したTRL用データ生成処理とは若干異なるTRL用データ生成処理を行い、コンテンツ鍵配信装置120は実施の形態2で示したTRL照合処理とは若干異なるTRL照合処理を行う。

【0101】<TRLの構成>図17は、実施の形態3におけるTRLのデータ構成を示す図である。同図では、端末数が数億台以上である場合に対応したTRLのデータ構成例を示している。同図に示すように、TRLは、8ビットのバージョン情報410と、128ビットの発行者情報420と、128ビットの無効化端末数430と、端末ID関連情報440と、320ビットの署名情報450とから構成される。

【0102】バージョン情報410、発行者情報420及び無効化端末数430は、実施の形態2で示したバージョン情報310、発行者情報320及び無効化端末数330と同一である。端末ID関連情報440は、128ビットのID442と8ビットのマスク用ビット443との組の1個又は複数個を含み、その個数を示すエントリ数441を含むところまでは、実施の形態2で示した端末ID関連情報340と同じであるが、更に128ビットの例外ID445を1個又は複数個含み、その個数を示す例外エントリ数444を含む。例外IDの数がM個であれば、例外エントリ数444の示す値はMとなる。

【0103】ここで、例外ID445は、無効化端末でない端末の端末IDである。この端末ID関連情報440では、ID442とマスク用ビット443との組により複数の端末の端末IDを包括的に表現するが、その組によって表現された端末IDのうち無効化端末IDでないものが、例外ID445によって示される。

【0104】従って端末ID関連情報440によれば、例えば仮に端末IDが4ビットであり、端末として端末0から端末15を想定した場合において、端末8～端末15のうち端末10を除く他のものは無効化端末である場合には、「1000」というID442と値が1であるマスク用ビット443との組と「1010」という例外IDとが端末ID関連情報の内容となる。

【0105】また、署名情報450は、バージョン情報410、発行者情報420、無効化端末数430及び端末ID関連情報440の全体を反映して作成されるいわゆるデジタル署名である。

<TRL用データ生成処理>図18は、実施の形態3における管理装置110により行われるTRL生成送信処理の一部であるTRL用データ生成処理を示すフローチャートである。

【0106】ここでは、端末IDをNビットであるとして説明する。Nは、例えば128ビットである。管理装置110においてTRL生成部112は、無効化端末ID群取得部111より無効化端末についての端末ID群を取得した後にTRL用データ生成処理を行う(図5参照)。

【0107】まず、TRL生成部112は、取得した端末ID群をメモリ等の記憶媒体の一領域である作業用ID領域に格納し(ステップS401)、各端末IDのう

ち、最下位ビットのみが異なる端末IDが作業用ID領域中に存在しないものについては、その最下位ビットのみが異なる端末IDを生成して作業用ID領域に格納するとともにその生成した端末IDを例外IDとして保存する(ステップS402)。

【0108】続いて、TRL生成部112は、メモリ等の記憶媒体の一領域である作業用ビット領域に1ビットのビットデータ「0」と「1」との2つを格納し(ステップS403)、変数Xに1を設定する(ステップS404)。ステップS404に続いて、TRL生成部112は、作業用ビット領域中、未着目のXビットのビットデータの1つに着目し(ステップS405)、作業用ID領域中に格納されている端末IDのうち、上位Xビットが着目中のビットデータと一致するという条件を満たすものの数をカウントする(ステップS406)。

【0109】ステップS406の結果、カウント数が2の(N-X)乗となった場合には(ステップS407)、TRL生成部112は、ステップS406におけるその条件を満たす端末IDを作業用ID領域から削除し(ステップS408)、その条件を満たす端末IDについて、変数Xの値をマスク用ビットとして、更に上位Xビット分を着目中のビットデータと同一にして他のビットを「0」としたNビットのビット列をIDとして、そのマスク用ビットとIDとを一組としてメモリ等の記憶媒体の一領域に保存し(ステップS409)、ステップS410の判断を行う。

【0110】また、ステップS406の結果、カウント数が2の(N-X)乗でない場合には(ステップS407)、TRL生成部112は、ステップS406におけるその条件を満たす端末IDのうち上位からX+1ビット目が「0」のものが2個以上存在すれば、着目中のビットデータの下位に1ビットの「0」を加えて形成されるビットデータを作業用ビット領域に格納し(ステップS411)、その条件を満たす端末IDのうち上位からX+1ビット目が「1」のものが2個以上存在すれば、着目中のビットデータの下位に1ビットの「1」を加えて形成されるビットデータを作業用ビット領域に格納し(ステップS412)、ステップS410の判断を行う。

【0111】ステップS410では、TRL生成部112は、未着目のXビットのビットデータが存在するか否かを判定し、未着目のXビットのビットデータが未だ存在すればステップS405に戻って次のビットデータに着目して処理を行い、未着目のXビットのビットデータが存在しなければ変数Xを1増加し(ステップS413)、変数XがNと等しいか否かを判定する(ステップS414)。

【0112】TRL生成部112は、ステップS414において変数XがNと等しくないと判定した場合には、再びステップS405に戻って次のビットデータに着目

10

20

30

40

50

して処理を行い、変数XがNと等しいと判定した場合には、TRL用データ生成処理を終了する。なお、実施の形態3においては、図5のステップS23で示すTRLの構築は、上述のTRL用データ生成処理によって記憶媒体の一領域に保存されたIDとマスク用ビットとの1個又は複数個の組にエントリ数を付加したものと、例外IDにエントリ数を付加したものと、更にバージョン、発行者情報、無効化端末数及び署名情報を加えることによって実行される。

【0113】<TRL照合処理>図19は、実施の形態3におけるコンテンツ鍵配信装置120により行われるコンテンツ鍵配信処理の一部であるTRL照合処理を示すフローチャートである。コンテンツ鍵配信装置120の照合部126は、端末から送られた端末IDを送信要求受付部125より得る度にこのTRL照合処理を行う。

【0114】照合部126は、端末から送られた端末IDと、TRLの端末ID関連情報中のIDとマスク用ビットとの組のいずれかで表される端末IDとが一致するかを検査する(ステップS421~S424)。即ち、照合部126は、TRL中の1つの未着目のマスク用ビットに着目し、そのマスク用ビットの値に応じたマスクデータを上述したように導出して(ステップS421)、端末から送られた端末IDと、導出したマスクデータとのビット毎の論理積を求めて(ステップS422)、求めた論理積が着目中のマスク用ビット443と組をなすID442と一致するか否かを判定する(ステップS423)。

【0115】ステップS423の判定の結果、一致する場合には、照合部126は、端末から送られた端末IDがTRL中の例外IDのいずれかと一致するかを検査し(ステップS426)、例外IDのいずれとも一致しなければ、端末から取得した端末IDは無効化端末の端末IDであると判定し(ステップS427)、TRL照合処理を終了する。ステップS426の検査の結果、例外IDのいずれかと一致すると判明した場合には、照合部126は、端末から取得した端末IDは無効化端末の端末IDでないと判定し(ステップS425)、TRL照合処理を終了する。

【0116】また、ステップS423において、求めた論理積が着目中のマスク用ビット443と組をなすID442と一致しない場合には、照合部126はTRL中の全てのマスク用ビット443に着目してステップS421~S423の処理を行なったかを判定し(ステップS424)、全てのマスク用ビット443に着目して処理を行っていない場合にはステップS421に戻って未着目のマスク用ビットに着目して処理を行う。

【0117】ステップS424において、全てのマスク用ビットについて処理済みであると判定した場合には、照合部126は、端末から取得した端末IDは無効化端

末の端末IDでないと判定し(ステップS425)、TRL照合処理を終了する。

<考察>実施の形態3に示したコンテンツ鍵配信システムによれば、例えば、その端末IDの上位のいくらかの桁数のビット列が同値であるところの連続したシリアル番号の数十台の端末のうち、数台を除く他の全てが無効化端末であるような場合において、その同値であるビット列を含むIDをTRLの端末ID関連情報中のIDとし、その同値である部分の桁数を示す値をそのIDと組をなすマスク用ビットとして定め、その数台についての端末IDを端末ID関連情報中の例外IDとして定めたTRLによって無効化端末を特定することが可能となるため、TRLのデータ量を少なく抑えることができるようになる。

<実施の形態4>以下、実施の形態4に係るコンテンツ鍵配信システムについて説明する。

【0118】図20は、本発明の実施の形態4に係るコンテンツ鍵配信システムの構成図である。実施の形態1で示したコンテンツ鍵配信システム100における管理装置110は、TRLを通信路を通じてコンテンツ鍵配信装置120に対して送信するものであったのに対し、この実施の形態4に係るコンテンツ鍵配信システム500においては管理装置510はTRLを光磁気ディスク等の記録媒体501に記録し、コンテンツ鍵配信装置520がその記録媒体501からTRLを読み出すようになっている。

【0119】図20においては、実施の形態1で示した構成要素(図1参照)と基本的に同等のものについては同一の符号を用いて表しており、その構成要素についてはここでは詳しく説明しない。管理装置510は、例えばコンテンツの著作権等の保護に関する業務を行う機関に設置されるコンピュータ等であり、各端末130のうち、内部に記憶されている復号鍵が暴露される等により著作権等の保護が図れない事態に陥っている全ての端末、即ち暗号化コンテンツ鍵の配信先にすべきでない全ての端末を、特定するための情報を主たる内容とするTRLを生成して記録媒体に記録する処理を行う装置であり、無効化端末ID群取得部111、TRL生成部112及びTRL記録部513を備え、光磁気ディスク等の記録媒体501を装着できる。

【0120】ここで、TRL生成部112は、無効化端末ID群取得部111から与えられた各端末IDに基づいて無効化端末を特定する情報を主たる内容とするTRLを生成し、TRL記録部513に伝える機能を有する。また、TRL記録部513は、TRL生成部112から伝えられたTRLを管理装置510に装着された記録媒体501に記録する機能を有する。

【0121】この管理装置510は、図5に示すステップS24をTRLを記録媒体に記録する処理に置き換えた内容のTRL生成送信処理を行う。管理装置510に

よってTRLが記録された記録媒体501は、人手を介してコンテンツ鍵配信装置520に配送される。例えば、新たな内容のTRLが生成される毎に、TRLは記録媒体に記録され、コンテンツ鍵配信装置まで配送される。

【0122】コンテンツ鍵配信装置520は、各端末からの暗号化コンテンツ鍵の送信要求を受けるとその端末が無効化端末でない場合に限りその端末に暗号化コンテンツ鍵を送信することを内容とするコンテンツ鍵配信処理を行うコンピュータであり、機能的には、TRL格納部121、TRL読出部522、コンテンツ鍵記憶部123、暗号化鍵群記憶部124、送信要求受付部125、照合部126、暗号化部127及び暗号化コンテンツ鍵送信部128を備え、光磁気ディスク等の記録媒体501を装着できる。

【0123】ここで、TRL読出部522は、コンテンツ鍵配信装置520に装着された記録媒体501からTRLを読み出してTRL格納部121に格納する機能を有する。従って、このコンテンツ鍵配信システム500においては、管理装置510とコンテンツ鍵配信装置520とが通信路で接続されていなくても、記録媒体を介してTRLの伝達が実現される。

【0124】なお、この実施の形態4において用いられるTRLは実施の形態1～3のいずれで示したものであってもよく、コンテンツ鍵配信装置がそのTRLの構造に応じたTRL照合処理等を行うこととすればよい。

<補足>以上、本発明に係る暗号通信システムについて、コンテンツ鍵配信システムとして適用した実施の形態1～4を示して説明したが、本発明はこのような実施の形態に限られないことは勿論である。即ち、

(1) 実施の形態1～3では、管理装置とコンテンツ鍵配信装置との間でTRLを配信するための通信路を示し、実施の形態4では、TRLの配送に用いる記録媒体を示したが、管理装置とコンテンツ鍵配信装置との間は、通信路と記録媒体とを合わせて用いることによってTRLが伝送されるようになっていてもよい。例えば、管理装置から別のある通信装置までは記録媒体でTRLが配送され、その通信装置からコンテンツ鍵配信装置までは通信路を通じてTRLが配信されることとしてもよい。

(2) 各実施の形態で示したコンテンツ再生装置は、必ずしも暗号化コンテンツを予め入手してからコンテンツ鍵配信装置に送信要求を送らなければならないのではなく、例えば、コンテンツ鍵を取得した後、暗号化コンテンツを入手してその再生を行うこととしてもよい。

(3) 各実施の形態で示したコンテンツ再生装置は、その装置固有の端末IDと、その装置固有の復号鍵を保持していることとし、コンテンツ鍵配信装置は全ての復号鍵に呼応する暗号化鍵を保持していることとしたがた、コンテンツ再生装置が複数の復号鍵を備え、各復号

鍵を識別するための復号鍵IDを送信要求に含めてコンテンツ鍵配信装置に送り、また、コンテンツ鍵配信装置は全ての復号鍵に呼応する暗号化鍵を復号鍵IDと対応付けて保持しておき、その送られた復号鍵IDに対応する暗号化鍵を用いてコンテンツ鍵をコンテンツ再生装置に送信することとしてもよい。なお、この場合には、各実施の形態で示したTRLの端末ID関連情報によって、無効化端末の端末IDの代わりに、無効化すべき復号鍵に対応する復号鍵IDを特定するようにし、TRL照合処理等において端末IDの代わりに復号鍵IDを照合対象とすることとすればよい。

【0125】なお、コンテンツ再生装置に着脱可能なICカード等に、復号鍵及び復号鍵IDが記録されていることとしてもよい。

(4) 実施の形態1～3では管理装置のTRL生成部112が、TRL用データ生成処理(図10、図14、図18)等によりTRLを自動生成することとしたが、TRLの端末ID関連情報を生成するアルゴリズムはこれに限定されることはない。また、TRLは、オペレータ等の入力操作を受けて生成されることとしてもよいし、また外部装置において生成されたTRLを管理装置内に取得してからTRL送信部113でそのTRLを配信することとしてもよい。

【0126】また、コンテンツ鍵配信システムにおいて管理装置が複数存在することとしてもよく、ある管理装置から他の管理装置にTRLを伝送しておくこととしてもよい。また、コンテンツ鍵配信装置の方から管理装置に要求を出したときに、管理装置がTRLの送信を行うこととしてもよく、コンテンツ鍵配信装置は定期的又は端末から送信要求があったときにTRLの送信を管理装置に要求することとしてもよい。

(5) 実施の形態2で示した端末IDのデータ構成は、必ずしも図12に示した内容である必要はない。但し、メーカーや、製品等を表すビット列を端末ID中に含ませておくことにより、あるメーカーの製造した端末全てが無効化端末となる場合等にTRLのデータ量を小さくすることができるようになる。

【0127】なお、実施の形態2では、上位のビット列でメーカーIDを表すものとして端末IDを定義した例を示したが、端末ID中の下位のビット列を、メーカーIDを表すものとして端末IDを定義してもよいし、端末ID中の上位と下位との間のビット列を、メーカーIDを表すものとして端末IDを定義してもよい。

(6) 実施の形態2で示したTRLの端末ID関連情報中のマスク用ビットは、例えば8ビット等と固定長データとしたが、可変長データとして、そのデータ長を示す情報と対にしておくこととしてもよい。

(7) 実施の形態3で示したTRL用データ生成処理の結果として得られた端末ID関連情報に関して、端末IDが128ビットとした場合において、例外IDから最

10

20

30

40

50

下位ビットを0としたIDとマスク用ビットが127という値を示す一組が端末ID関連情報中に存在するときには、その一組及びその例外IDを削除して、その例外IDの最下位ビットを反転したものをIDとしてマスク用ビットを128とした一組を端末ID関連情報中に追加することとしてもよい。

【0128】また、実施の形態3では、各例外IDは、1つの端末IDを示すものとしたが、図17に示した例外IDの代わりに、例外IDと例外マスク用ビットとの組を1個又は複数個含む例外グループ情報をTRLの端末ID関連情報中に含めることとしてもよい。即ち、ID442とマスク用ビットとの組の全てで示される端末ID群の中から、その例外IDと例外マスク用ビットとの組の全てで示される端末ID群を除いたものが、全ての無効化端末の端末IDであるように端末ID関連情報を構成することとしてもよい。

(8) 実施の形態1～4では、本発明に係る暗号通信システムが、コンテンツ鍵配信システムに適用された場合の例を示したが、端末からの端末IDを受けてその端末が無効化端末か否かを判定してその判定結果に応じて何らかの通信処理の実行可否を決定するような通信システムであれば、特にその通信処理内容は、暗号化コンテンツ鍵の送信に限るものではない。例えば、無効化端末か否かの判定の結果に応じて、端末側から端末固有の暗号化を施して送られる重要データを受け付ける処理の実行可否を決定することとしてもよい。

(9) 実施の形態1～3で示したコンテンツ鍵配信システムの処理手順(図5～7、図10、図11、図14、図16、図18、図19に示した手順等)を、コンピュータ等に実行させるためのコンピュータプログラムを、記録媒体に記録し又は各種通信路等を介して、流通させ頒布することもできる。このような記録媒体には、ICカード、光ディスク、フレキシブルディスク、ROM等がある。流通、頒布されたコンピュータプログラムは、コンピュータ等にインストール等されることにより利用に供され、そのコンピュータ等は当該コンピュータプログラムを実行して、実施の形態1～3で示したような各種処理を行うことができるようになる。

【0129】

【発明の効果】以上の説明から明らかなように、本発明に係る暗号通信システムは、暗号通信装置と、自端末装置を識別可能な所定ビット数のビット列なる端末識別子を、当該暗号通信装置に送信する機能を有する複数の端末装置と、無効化すべき端末装置を特定するものとして1以上の端末識別子を示す無効化端末特定情報を生成する管理装置とを備える暗号通信システムであって、前記管理装置は、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定

情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを有し、前記暗号通信装置は、前記管理装置により出力された前記無効化端末特定情報を取得する無効化端末特定情報取得手段と、端末装置から端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、一方、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを有することを特徴とする。

【0130】ここで、暗号通信装置は、例えば実施の形態1～3で示すようなコンテンツ鍵配信装置であり、所定の通信とは例えば暗号化コンテンツ鍵の送信であり、無効化端末特定情報は例えば実施の形態1～3において示すTRLである。本発明により、あるビット列を含む全ての端末IDを、それに含まれる共通するビット列の値と位置とを特定する情報で包括的に表現するので、TRLのデータ量を比較的小さく抑えることができるようになり、この結果、一部の無効化すべき端末装置を除いた適切な端末装置に対してのみ、コンテンツ鍵を暗号化して配信する等の暗号通信に係るサービスを行う実用的な暗号通信システムが実現される。

【0131】また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて1組以上含んでおり、端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各位置情報について、前記端末識別子受信手段により受信された端末識別子中の当該位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定する



こととしてもよい。

【0132】これにより、無効化端末特定情報を、端末IDの一部の値とそ一部の位置とを対応付けている形式としたため、一部の位置を運用ルール等で固定的に決めておく必要なく、任意のビット列範囲についてその範囲の値が共通な全ての端末IDを一組の値及び位置からなる情報で表し得るため、効果的に運用すれば、多数の無効化端末を少ない情報量で表すことができるようになる。

【0133】また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列である代表値情報と、所定ビット数のマスクフラグとを対応付けて1組以上含んでおり、端末識別子中の部分のうち各マスクフラグにおけるビット値が1である部分の値が、当該マスクフラグに対応する代表値情報における当該部分の値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各マスクフラグについて、前記端末識別子受信手段により受信された端末識別子と当該マスクフラグとの論理積と、当該マスクフラグに対応する代表値情報と当該マスクフラグとの論理積とが一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【0134】これにより、端末IDの一部の値とそ一部のビット位置との組で、多数の端末IDを表す方式において、その一部を構成するビット位置を、マスクフラグ中の値を1とした位置で示して、その一部を構成しないビット位置を、マスクフラグ中の値を0とした位置で示すことになる。従って、端末から受信した端末IDのうち、無効化端末特定情報中に含まれる値と照合すべき部分を、その端末IDとマスクフラグとの論理積を求めるという計算量の小さい簡易な演算によって抽出することができるようになる。このことは、暗号通信装置における判定の高速化につながる。

【0135】また、前記無効化端末特定情報生成手段は、前記無効化端末特定情報に所定ビット数の孤立値情報を含めて生成し、前記無効化端末特定情報は、更に前記孤立値情報と同一の値を有する端末識別子をも、無効化すべき端末装置として特定する情報であり、前記判定手段は更に、前記端末識別子受信手段により受信された端末識別子と、前記無効化端末特定情報に含まれる孤立値情報とが一致する場合にも、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【0136】ここで孤立値情報は、例えば図8で示す個

別情報であり、これにより、一の無効化端末の端末IDが、他の無効化端末の端末IDと共通するビットを持たない場合、つまり孤立している場合において、その一の無効化端末の端末IDを孤立値情報として無効化端末特定情報に含ませているため、孤立した無効化端末が多い場合には、その一の無効化端末の端末IDを、その端末IDの値と全ビットが1であるマスクフラグとの組で表現した形式よりも、少量のデータで無効化端末特定情報を構成することができる。

【0137】また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、ビット桁数を示す有効上位桁情報と、当該ビット桁数分のビット列の値を示す値情報とを対応付けて1組以上含んでおり、端末識別子中の最上位ビットから各有効上位桁情報により示されるビット桁数分のビット列の値が、当該有効上位桁情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各有効上位桁情報について、前記端末識別子受信手段により受信された端末識別子中の最上位ビットから当該有効上位桁情報により示されるビット桁数分のビット列の値が、当該有効上位桁情報に対応する値情報で示される値と一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【0138】これにより、端末IDの上位から任意のビット数分だけ共通な値を持つ全ての端末IDを、そのビット数を示す有効上位桁情報と値情報とにより表すことができる。一般に端末IDの管理運用上、端末を製造したメーカー識別子等、ある程度端末の構造や機能に共通な性質を有するまとまりを区別する情報が端末IDの上位ビットに位置付けることが多いことから、これにより、特定のメーカーや製品構造等に関連して無効化すべき端末が多数発生した場合において、比較的少量のデータで無効化端末特定情報を構成することができるようになる。

【0139】また、前記管理装置は、無効化すべき全ての端末装置の端末識別子を取得する端末識別子取得手段を有し、前記無効化端末特定情報生成手段は、前記所定ビット数をNとすると、前記端末識別子取得手段により取得された端末識別子のうち最上位ビットからXビットの値が同一である端末識別子の個数が2の(N-X)乗であるという条件を満たすXの値を1以上特定し、各Xの値について、当該条件に係る2の(N-X)乗個の端末識別子を、Xなるビット桁数を示す有効上位桁情報と、当該端末識別子の最上位ビットからXビットの部分のビット列の値を示す値情報とをもって包括的に表現し

たデータ形式を用いて前記無効化端末特定情報を生成することとしてもよい。

【0140】これにより、管理装置のオペレータ等に特段の操作負担をかけることなく、データ量を抑えた無効化端末特定情報を構築することができるようになる。また、前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すこととしてもよい。

【0141】これにより、上位から一定のビット数分が共通である全ての端末IDを一組の小さな情報で表すことが可能であり、端末IDの上位にメーカーを示す情報が含まれるため、特定のメーカーが製造した端末に機構上の問題、例えばユーザが一定手順を実行することにより無制限にコンテンツをコピーできるような欠陥があることが判明した場合等において、無効化端末特定情報のデータ量を効果的に抑えることができるようになる。

【0142】また、前記各端末装置を識別する各端末識別子は、当該端末識別子中の前記製造者を示すビット列に続く上位の所定数のビット列で、当該端末装置が如何なる種類の製品に属するかを示すこととしてもよい。これにより、特定メーカーの製造した一定の製品のみの問題があることが判明した場合において、その製品が実装された全ての端末を無効化端末とするために必要な無効化端末特定情報のデータ量を抑えることが可能となる。

【0143】また、前記複数の端末装置は各々固有の復号鍵を保持しており、更にコンテンツ鍵で暗号化されたコンテンツである暗号化コンテンツを自端末装置内部に格納可能であり、前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、前記暗号通信装置は、全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段と、前記コンテンツ鍵を記憶するコンテンツ鍵記憶手段とを有し、前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行い、前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて前記コンテンツ鍵を暗号化して送信し、前記端末装置は、暗号通信装置から送信された暗号化済みのコンテンツ鍵を自端末装置固有の前記復号鍵を用いて復号する復号手段と、前記暗号化コンテンツが自端末装置内部に格納されている場合において前記復号手段により復号されたコンテンツ鍵を用いて当該暗号化コンテンツを復号して再生する再生手段とを有することとしてもよい。

【0144】これにより、端末は暗号化コンテンツ鍵を

暗号通信装置から取得した場合に限ってコンテンツの再生が可能になることとして著作権保護等に配慮したシステムを実現する場合において、あるメーカーの製造した一群の端末が著作権保護不可能な状態に陥ったことが判明したときに、端末ID中の上位からメーカーIDの部分までを示すビット桁数及びそのメーカーIDという少ないデータ量のデータでその一群の無効化すべき端末を識別するための情報を構成することができるため、管理装置から暗号通信装置に送信しなければならないデータのデータ量を抑えることができ、そのデータの送信時間が短縮できる。

【0145】また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値及び当該部分を特定する包括情報を1以上含み、かつ、所定ビット数の例外情報を1以上含んでおり、端末識別子中の部分のうち各包括情報により特定される部分が当該包括情報により特定される値と同一である全ての端末識別子のうちから、前記各例外情報と同値である端末識別子を除いたものの全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記端末識別子受信手段により受信された端末識別子が、前記無効化端末特定情報に含まれるいずれかの包括情報により特定される部分において当該包括情報により特定される値と一致するか否かを検査し、当該検査において一致した場合には、当該受信された端末識別子が前記無効化端末特定情報に含まれるいずれかの例外情報と同値である場合を除いて、当該端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【0146】これにより、単に包括情報のみで無効化端末の端末IDを特定するより、例外情報を用いていることによって、少ないデータ量で全ての無効化端末の端末IDを特定することができる場合がある。例えば、無効化端末が15台あり、その端末IDはいずれも下位4ビットを除く全てのビット列の値が共通している状況を想定すれば、仮に、1つの包括情報によって、下位3ビットを除く全てのビット列の値が共通する8個の端末IDを表現し、別の1つの包括情報によって、下位2ビットを除く全てのビット列の値が共通する4個の端末IDを表現し、更に別の1つの端末IDの値自体によってその端末IDを表現することとして合計15台の無効化端末の端末IDを特定する無効化端末特定情報を構築する場合に比べて、本発明によれば、例えば1つの包括情報によって、下位4ビットを除くビット列が共通する16個の端末IDを表現し、例外情報によって、その16個の端末IDのうち無効化端末でない1台の端末の端末IDを表現することとして同じ意味の無効化端末特定情報を構築することができるので、無効化端末特定情報のデータ量を抑えることができる。

【0147】また、前記管理装置は、無効化すべき全ての端末装置の端末識別子を取得する端末識別子取得手段を有し、前記無効化端末特定情報生成手段は、前記所定ビット数を $N$ とすると、前記端末識別子取得手段により取得されたいずれかの端末識別子の最下位ビットのみ反転した $N$ ビットのビット列であって、当該端末識別子取得手段により取得された他のいずれかの端末識別子とも値が同一でないという条件を満たすビット列を、前記例外情報と定めるとともに、当該ビット列を端末識別子とみなし、前記端末識別子取得手段により取得された端末識別子及び前記みなした端末識別子のうち、最上位ビットから $X$ ビットの値が同一である端末識別子の個数が2の $(N-X)$ 乗であるという条件を満たす $X$ の値で、かつ、 $N$ 未満である $X$ の値を、1以上特定し、特定した各 $X$ の値について、当該 $X$ の値と、当該条件に係る2の $(N-X)$ 乗個の端末識別子の最上位ビットから $X$ ビットの部分のビット列の値とを特定する情報を前記包括情報と定めることにより前記無効化端末特定情報を生成することとしてもよい。

【0148】これにより、管理装置のオペレータ等に特定の操作負担をかけることなく、一定の状況においてデータ量を抑えた無効化端末特定情報を構築することができるようになる。また、前記複数の端末装置は各々固有の復号鍵を保持しており、前記暗号通信装置は、全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段を有し、前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて通信データを暗号化して送信し、前記端末装置は、暗号通信装置から送信された通信データを自端末装置固有の前記復号鍵を用いて復号することとしてもよい。

【0149】これにより、正常な端末に対してのみに、通信データを送信するサービスを行う暗号通信装置を含むシステムにおいて、無効化すべき端末が多数発生したような事態においても、端末が正常なものであるか否かの判断に必要な無効化端末特定情報のデータ量を小さく抑えることができるため、その判断の迅速化等が図れるようになる。

【0150】また、前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行うこととしてもよい。これにより、管理装置は、暗号通信装置が必要とする無効化端末特定情報をデータ量を抑えて構築して、迅速に暗号通信装置に伝送することが可能になる。

【0151】また、前記出力手段は、記録媒体を装着可

能な装着部を有し、装着された記録媒体に前記無効化端末特定情報を記録することにより前記出力を行い、前記無効化端末特定情報取得手段は、前記記録媒体を装着可能であり、装着された記録媒体から前記無効化端末特定情報を読み出すことにより前記取得を行うこととしてもよい。

【0152】これにより、管理装置が、暗号通信装置が必要とする無効化端末特定情報を記録媒体に記録して伝達する場合において、ある程度小さい記録許容容量の従来の記録媒体を利用することができるようになる。また、本発明に係る管理装置は、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき1以上の各端末装置の各端末識別子を示す無効化端末特定情報を生成する管理装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを備えることを特徴とする。

【0153】この管理装置によって、出力される無効化端末特定情報は比較的小さいデータ量で多数の無効化端末を特定することができるものとなり、その出力される無効化端末特定情報は、伝送や記録媒体への記録の面において、利用しやすいものとなる。また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて1組以上含んでおり、端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であることとしてもよい。

【0154】これにより、無効化端末特定情報を、端末IDの一部の値とその一部の位置とを対応付けている形式としたため、一部の位置を運用ルール等で固定的に決めておく必要なく、任意のビット列範囲についてその範囲の値が共通な全ての端末IDを一組の値及び位置からなる情報で表し得るため、効果的に運用すれば、多数の無効化端末を少ない情報量で表すことができるようになる。

【0155】また、前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、前記各端末装置を識別する各端末識別子は、当該端末識別子中の所定範囲のビット列で当該端末装置の製造者を示すこととしてもよい。これにより、特定のメーカーが製造した端末に機構上の欠陥あることが判明した場合等において、無効化端末特定情報のデータ量を効果的に抑えることが

できるようになる。

【0156】また、本発明に係る暗号通信装置は、複数の端末装置のうち自端末装置を識別可能な所定ビット数のビット列なる端末識別子を保持する各端末装置との間で通信を行う暗号通信装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて構成され、無効化すべき端末装置を特定するためのものとして1以上の各端末装置の各端末識別子を示した無効化端末特定情報を外部から取得する無効化端末特定情報取得手段と、端末装置から、当該端末装置が保持する端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを備えることを特徴とする。

【0157】これにより、比較的小さいデータ量で多数の無効化端末を特定する無効化端末特定情報を取得して参照し、端末から受信した端末IDが無効化端末の端末IDであるか否かの判定を迅速に行うことができるようになる。また、前記無効化端末特定情報取得手段により取得される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて1組以上含んでおり、端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各位置情報について、前記端末識別子受信手段により受信された端末識別子中の当該位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【0158】これにより、無効化端末特定情報を、端末IDの一部の値とその一部の位置とを対応付けている形式としたため、一部の位置を運用ルール等で固定的に決めておく必要なく、任意のビット列範囲についてその範囲の値が共通な全ての端末IDを一組の値及び位置からなる情報で表し得るため、効果的に運用すれば、多数の無効化端末を少ない情報量で表すことができるようになる。

【0159】また、本発明に係る情報生成方法は、複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成方法であって、前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップとを含むことを特徴とする。

【0160】これにより、多数の無効化端末を特定するための情報を小さいデータ量に抑えて構築することができるようになる。また、本発明に係る記録媒体は、無効化端末特定データを記録したコンピュータ読み取り可能な記録媒体であって、前記無効化端末特定データは、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を特定するために、前記所定ビット数のビット列中の一部分の値を特定するための部分特定情報を記録した端末識別子特定フィールドを有し、当該部分特定情報により、当該部分が当該値と同一である全ての端末識別子を包括的に表現していることを特徴とする。同様に、本発明に係る無効化端末特定データは、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を特定するために、前記所定ビット数のビット列中の一部分の値を特定するための部分特定情報を記録した端末識別子特定フィールドを有し、当該部分特定情報により、当該部分が当該値と同一である全ての端末識別子を包括的に表現していることを特徴とする。

【0161】これらにより、あるビット列を含む全ての端末IDを、それに含まれる共通するビット列の値と位置とを特定する情報で包括的に表現するので、無効化端末特定データのデータ量を比較的小さく抑えることができるようになる。また、本発明に係る暗号通信システムは、暗号通信装置と、当該暗号通信装置に所定ビット数の鍵識別子を送信する端末装置と、無効化すべき1以上の各鍵識別子を特定する無効化鍵識別子特定情報を生成する管理装置とを備える暗号通信システムであって、前記管理装置は、前記所定ビット数のビット列中の一部分

の値を特定する情報により当該部分が当該値と同一である全ての鍵識別子を包括的に表現するデータ形式を用いて、前記無効化鍵識別子特定情報を生成する無効化鍵識別子特定情報生成手段と、生成された前記無効化鍵識別子特定情報を出力する出力手段とを有し、前記暗号通信装置は、前記管理装置により出力された前記無効化鍵識別子特定情報を取得する無効化鍵識別子特定情報取得手段と、端末装置から鍵識別子を受信する鍵識別子受信手段と、前記鍵識別子受信手段により受信された鍵識別子が、前記無効化鍵識別子特定情報により特定される何れかの鍵識別子と一致するか否かを判定する判定手段と、前記受信された鍵識別子が前記無効化鍵識別子特定情報により特定される何れの鍵識別子とも一致しないと前記判定手段により判定された場合に限り、当該鍵識別子を送信した端末装置との間で、当該鍵識別子について固有な暗号化を施すことにより所定の通信を行う通信手段とを有することを特徴とする。

【0162】これにより、正当な鍵識別子を送った端末に対してのみ、特定の重要なデータの送信等といった所定の通信を行うようなサービスを行うシステムにおける、鍵識別子の正当性の確認に要するデータのデータ量を抑えることができるので、かかるシステムの実用性を高めることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態1に係るコンテンツ鍵配信システムの構成図である。

【図2】各端末が記憶している端末IDと復号鍵とを示す図である。

【図3】各端末が保持する端末IDの値の決定方法を示す概念図である。

【図4】コンテンツ鍵配信装置120の暗号化鍵群記憶部124に記憶されるデータの内容例を示した図である。

【図5】管理装置110が行うTRL生成送信処理を示すフローチャートである。

【図6】コンテンツ再生装置130が行うコンテンツ再生処理を示すフローチャートである。

【図7】コンテンツ鍵配信装置120が行うコンテンツ鍵配信処理を示すフローチャートである。

【図8】実施の形態1におけるTRLのデータ構成を示す図である。

【図9】TRLの内容例を示す図である。

【図10】実施の形態1における管理装置110により行われるTRL生成送信処理の一部であるTRL用データ生成処理を示すフローチャートである。

【図11】実施の形態1におけるコンテンツ鍵配信装置120により行われるコンテンツ鍵配信処理の一部であるTRL照合処理を示すフローチャートである。

【図12】実施の形態2における端末IDのデータ構成を示す図である。

【図13】実施の形態2におけるTRLのデータ構成を示す図である。

【図14】実施の形態2における管理装置110により行われるTRL生成送信処理の一部であるTRL用データ生成処理を示すフローチャートである。

【図15】TRLの内容例を示す図である。

【図16】実施の形態2におけるコンテンツ鍵配信装置120により行われるコンテンツ鍵配信処理の一部であるTRL照合処理を示すフローチャートである。

10 【図17】実施の形態3におけるTRLのデータ構成を示す図である。

【図18】実施の形態3における管理装置110により行われるTRL生成送信処理の一部であるTRL用データ生成処理を示すフローチャートである。

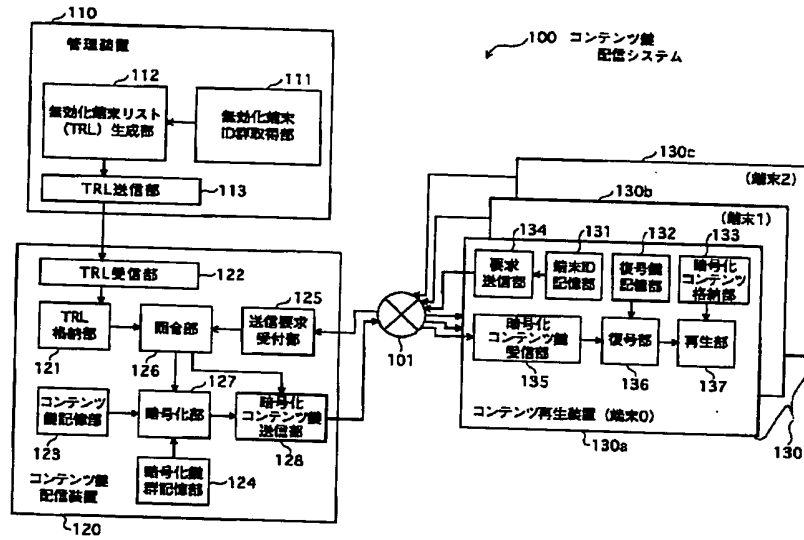
【図19】実施の形態3におけるコンテンツ鍵配信装置120により行われるコンテンツ鍵配信処理の一部であるTRL照合処理を示すフローチャートである。

【図20】本発明の実施の形態4に係るコンテンツ鍵配信システムの構成図である。

20 【符号の説明】

100	コンテンツ鍵配信システム
101	通信路
110	管理装置
111	無効化端末ID群取得部
112	TRL生成部
113	TRL送信部
120	コンテンツ鍵配信装置
121	TRL格納部
122	TRL受信部
30 123	コンテンツ鍵記憶部
124	暗号化鍵群記憶部
125	送信要求受付部
126	照合部
127	暗号化部
128	暗号化コンテンツ鍵送信部
130	コンテンツ再生装置（端末）
131	端末ID記憶部
132	復号鍵記憶部
133	暗号化コンテンツ格納部
40 134	要求送出部
135	暗号化コンテンツ鍵受信部
136	復号部
137	再生部
500	コンテンツ鍵配信システム
501	記録媒体
510	管理装置
513	TRL記録部
520	コンテンツ鍵配信装置
522	TRL読出部

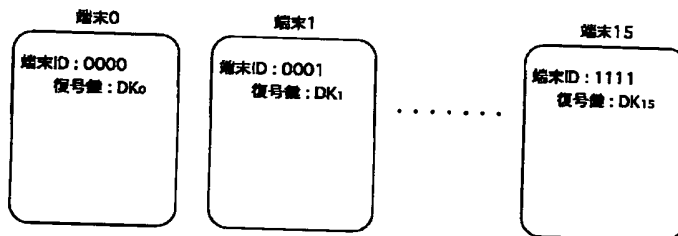
【図1】



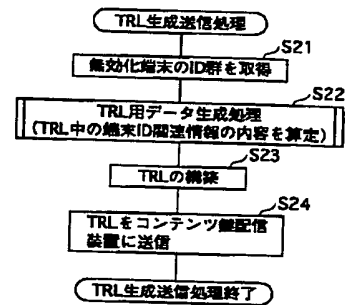
【図4】

暗号化鍵群記憶部	
端末ID	暗号化鍵
0000	EK <sub>0</sub>
0001	EK <sub>1</sub>
0010	EK <sub>2</sub>
...	...
1111	EK <sub>15</sub>

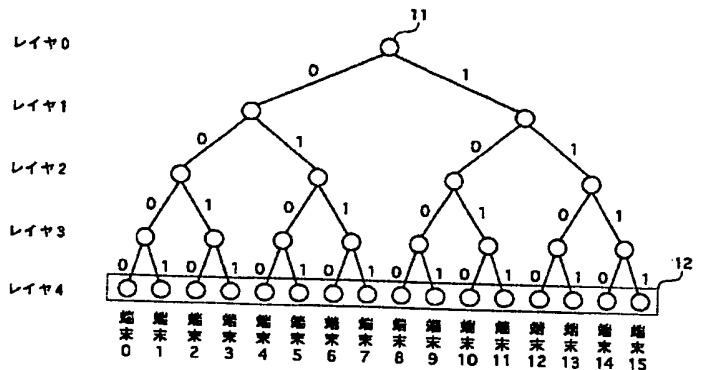
【図2】



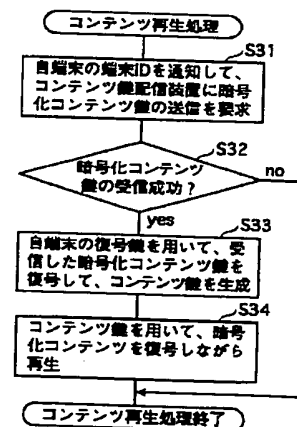
【図5】



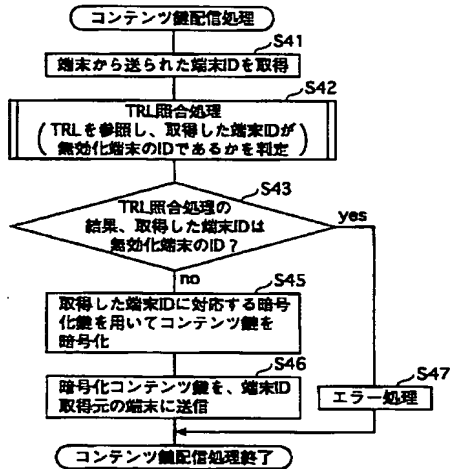
【図3】



【図6】



【図7】



【図9】

TRL 内容例			内容例
フィールド			
バージョン情報			1
端末ID関連情報	グループ情報	エントリ数	2
		ID	'1100'b
		マスクデータ	'1100'b
		ID	'0110'b
	マスクデータ	'1110'b	
	個別情報	エントリ数	1
ID		'0001'b	
署名情報			(上の全フィールドの内容を反映した値)

【図12】

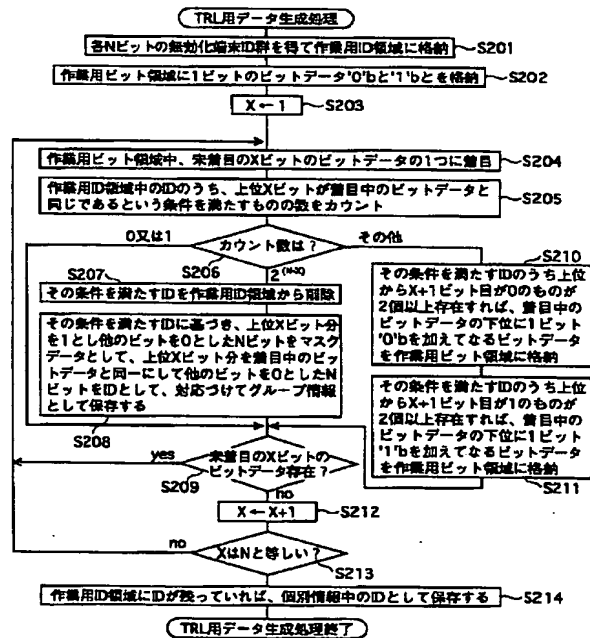
端末ID (128ビット)

フィールド	ビットサイズ	ビット位置
301 メーカーID	32	0~31
302 製品ID	32	32~63
303 製品バージョンID	32	64~95
304 シリアル番号	32	96~127

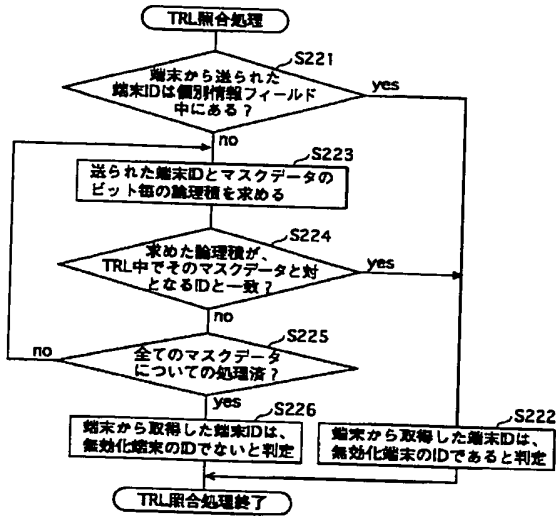
【図8】

TRL				
フィールド			ビットサイズ例 (他の例)	
210	バージョン情報		8 (8)	
220	端末ID 関連情報	グループ 情報	エントリ数 (M)	4 (128)
		個別 情報	M × { ID マスクデータ	4 (128)
				4 (128)
	221	個別 情報	エントリ数 (N)	4 (128)
225	署名情報	N × ID	4 (128)	
		署名情報	64 (320)	
230	署名情報		64 (320)	

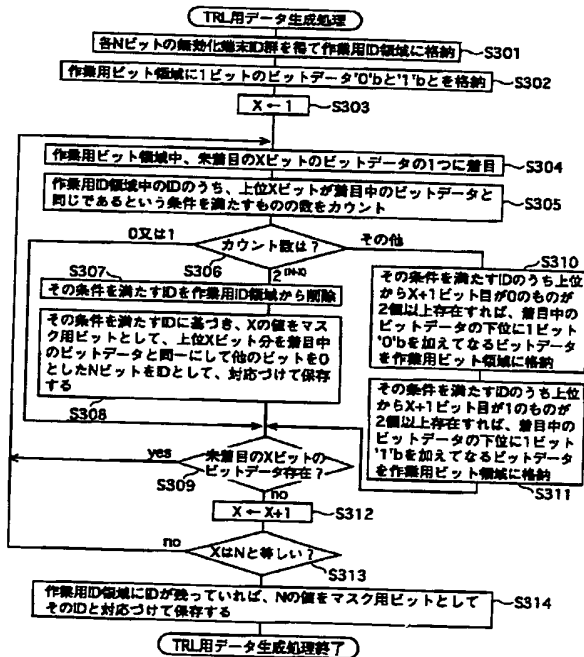
【図10】



【図11】



【図14】



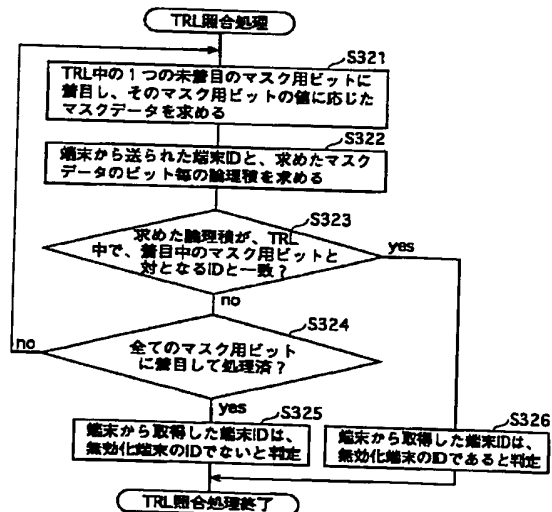
【図13】

TRL		フィールド	ビットサイズ
310		バージョン	8
320		発行者情報	128
330		無効化端末数	128
340	端末ID	エントリ数 (N)	32
	関連情報	ID	128
		マスク用ビット	8
350		署名情報	320

【図15】

TRL内容例		フィールド	内容例	ビットサイズ
		バージョン	1	8
		発行者情報	ABC	128
		無効化端末数	7	4
端末ID 関連情報	エントリ数	3	4	
	ID	'1100'b	4	
	マスク用ビット	2	2	
	ID	'0110'b	4	
	マスク用ビット	3	2	
	ID	'0001'b	4	
	マスク用ビット	4	2	
署名情報				320

【図16】

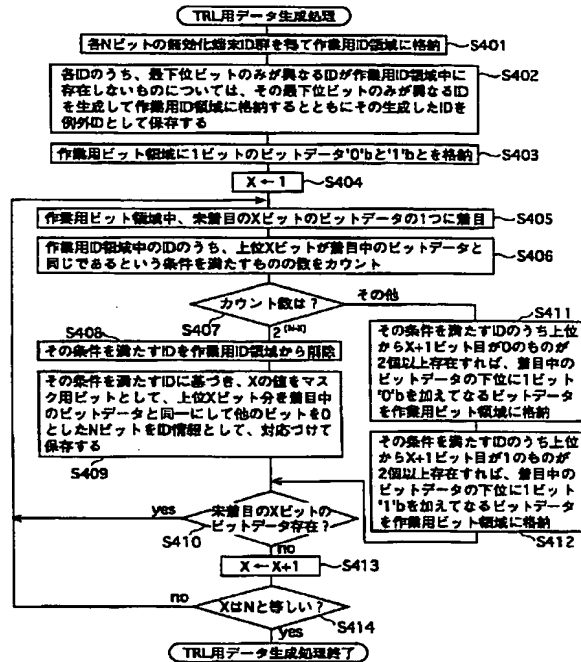




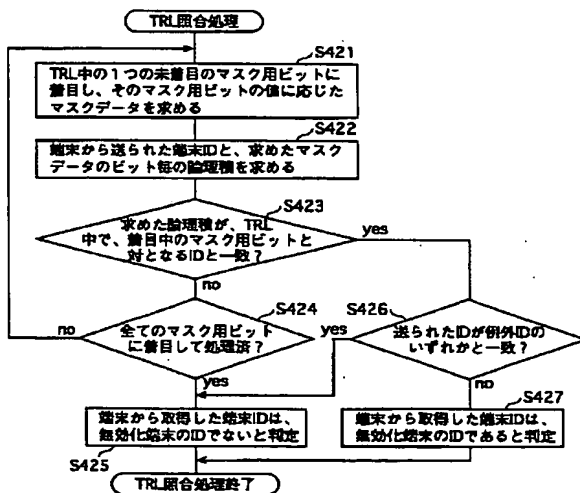
【図17】

TRL		フィールド	ビットサイズ
410		バージョン	8
420		発行情報	128
430		無効化端末数	128
440	端末ID 関連情報	エン트리数 (N)	32
		N × { ID マスク用ビット }	128
			8
		例外エン트리数 (M)	32
450		MX例外ID	128
		署名情報	320

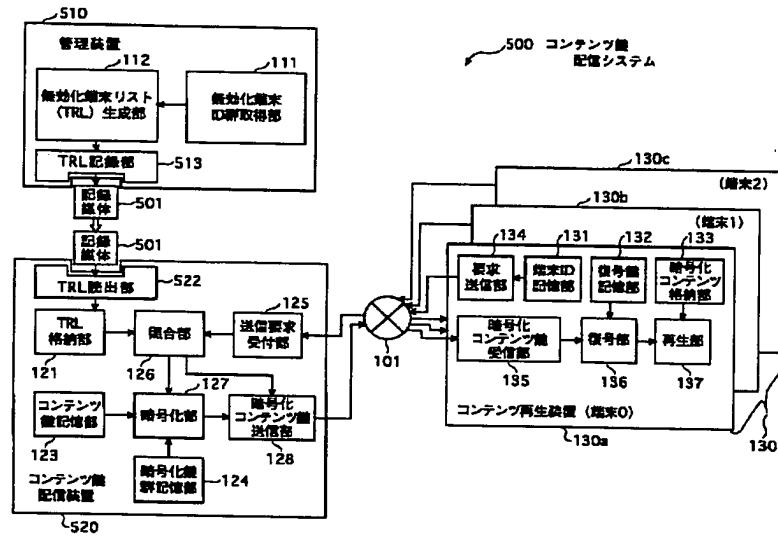
【図18】



【図19】



【図20】



フロントページの続き

(72)発明者 館林 誠  
 大阪府門真市大字門真1006番地 松下電器  
 産業株式会社内

F ターム(参考) 5J104 AA07 AA16 EA04 EA07 EA18  
 JA03 JA21 KA02 KA05 KA15  
 MA01 NA02 NA03 NA27

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)